JP00/6355

PCT/JP00/06355

28.09.00

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

22/3

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

EJV

出願年月日
Date of Application: １９９９年　９月１６日

出願番号
Application Number: 平成１１年特許願第２６２７６６号

出願人
Applicant (s): 松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年　９月１８日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０７５４７６

【書類名】　特許願

【整理番号】　2030714027

【提出日】　平成11年 9月16日

【あて先】　特許庁長官殿

【国際特許分類】　H04M 15/00

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地
松下電器産業株式会社内

【氏名】　高山　久

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地
松下電器産業株式会社内

【氏名】　松瀬　哲朗

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地
松下電器産業株式会社内

【氏名】　川口　京子

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地
松下電器産業株式会社内

【氏名】　中西　良明

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地
松下電器産業株式会社内

【氏名】　佐々木　理

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100082692

【弁理士】

【氏名又は名称】　蔵合　正博

【電話番号】　03(3519)2611

【手数料の表示】

【予納台帳番号】　013549

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9004843

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子財布

【特許請求の範囲】

【請求項１】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項２】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項１記載の電子財布。

【請求項３】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項４】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項３記載の電子財布。

【請求項５】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項６】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項５記載の電子財布。

【請求項７】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された属性情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項８】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項７記載の電子財布。

【請求項９】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項１０】　前記電子情報から電子情報オブジェクトを生成し前記電子情

報を制御する手段を備えた請求項９記載の電子財布。

【請求項１１】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項１２】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項１１記載の電子財布。

【請求項１３】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報の識別情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項１４】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項１３記載の電子財布。

【請求項１５】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項１６】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項１５記載の電子財布。

【請求項１７】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項１８】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項１７記載の電子財布。

【請求項１９】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項２０】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項１９記載の電子財布。

【請求項２１】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報と表示リソースの識別情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項２２】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項２１記載の電子財布。

【請求項２３】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及びサービス制御情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項２４】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項２３記載の電子財布。

【請求項２５】　少なくとも一組以上の固有の秘密鍵とその証明書の組と、少なくとも一つ以上の前記秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報と表示リソースの識別情報と電子情報ハンドラの認証鍵及びサービス制御情報とを備えた電子情報を保存管理する手段を備えた電子財布。

【請求項２６】　前記電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を備えた請求項２１記載の電子財布。

【請求項２７】　前記電子情報を構成する前記サービス制御情報が、少なくとも一つ以上のサービス制御モジュール情報の組合せであることを特徴とする請求項２３から請求項２６記載の電子財布。

【請求項２８】　前記電子情報の電子情報オブジェクトが、決済処理時に交換する各メッセージに、前記サービス制御情報に基づく決済データを重畳することを特徴とする請求項２３から請求項２６記載の電子財布。

【請求項２９】　前記電子情報の電子情報オブジェクトが、決済処理時に交換

する各メッセージに、前記サービス制御モジュール情報の組合せに基づく決済データを重畳することを特徴とする請求項２７記載の電子財布。

【請求項３０】　前記電子情報の電子情報オブジェクトが、決済データを重畳するメッセージが、電子情報から電子情報ハンドラに決済処理を申し出るメッセージと、電子情報ハンドラから電子情報に属性値の変更を命令するメッセージと、電子情報から電子情報ハンドラに属性値の変更結果を示すメッセージと、電子情報ハンドラから電子情報への領収書に相当するメッセージであることを特徴とする請求項２８または請求項２９記載の電子財布。

【請求項３１】　前記電子情報の表示手段を備えることを特徴とする請求項１から請求項３０記載の電子財布。

【請求項３２】　前記電子情報から表示情報を生成する手段を備えることを特徴とする請求項１から請求項３０記載の電子財布。

【請求項３３】　請求項１から請求項３２に記載の前記電子財布の処理プログラムを、電子計算機が読み取り可能な形式で記録した処理プログラム記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、プリペイドカードやクレジットカード（バンクカード）に代表される小売販売取引における決済機能、各種イベント、公演、映画等のチケットの改札機能、さらには、それら、プリペイドカードやチケットの流通・販売機能を提供するエレクトロニックコマースシステムに関し、特に、利便性と、決済の安全性を担保し、効率的で、円滑な商取引を可能にするものである。

【０００２】

【従来の技術】

近年、電子マネーや電子チケットなど価値情報を電子化し、流通を効率化しようとする取り組が行われている。

その一つの方式として、その価値情報が持つ属性をマークアップ記述言語で規定して、それに所有者のデジタル署名を施すことによって、流通を可能にする方式がある。図２１（ａ）は、従来の技術における価値情報の発行者のセンターサー

バ２１００からユーザのＩＣカード２１０１に、電子化された価値情報２１０３が発行された状態を示す模式図である。ＩＣカード２１００に格納された価値情報２１０３は、マークアップ記述言語によって、価値情報が持つ属性が記述されており、不正な改竄を防止するため、全体に対して発行者(Issuer)によるデジタル署名が施されている。また、図２１（ｂ）は、従来の技術における電子化された価値情報２１０３がマーチャントに対して使用された状態を示す模式図である。マーチャント端末２１０２に格納されている価値情報２１０４は、ＩＣカード２１００に格納されていた価値情報２１０３に、所有者の変更を示す情報を付加し、不正な改竄を防止するため、ユーザ(User)によるデジタル署名が施されたものである。情報は変更せず、追加するだけなので、改竄等の不正行為に対す安全性が高く、電子化された価値情報を安全に流通させることが出来る方式である。

【０００３】

【発明が解決しようとする課題】

しかしながら、従来の方式では、電子化された価値情報が流通する度に、電子化された価値情報のデータサイズが大きくなってしまい、取り扱いが不便であった。また、従来の方式では、電子化された価値情報を流通させる時に、双方の証明書を交換してデジタル署名を検証する必要があり、匿名性が確保できないという課題があった。さらに、従来の方式では、価値情報の種類により電子化の方式が異なり、例えば、プリペイドカードやチケットを統一的に取り扱うことができないという課題があった。

【０００４】

本発明は、こうした従来の技術の課題を解決するもので、匿名性と安全性、および利便性に優れ、価値情報の効率的な電子化と、各種の電子化された価値情報をユーザが効率的に取り扱うことが出来る電子財布を提供することを目的としている。

【０００５】

【課題を解決するための手段】

これらの課題を解決するために本発明は、第１に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された情報とを備えた電子情報を、保存管理す

る手段を電子財布に備えたものである。電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

【０００６】

第２に、第１の電子財布に、電子情報から電子情報オブジェクトを生成し電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【０００７】

第３に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

【０００８】

第４に、第３の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【０００９】

第５に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の発行者が規定する情報を、電子情報に入れることが出来る。

【００１０】

第６に、第５の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００１１】

第７に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された属性情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の属性情報の有効性がそれ自身で証明されるので、匿名性が確保される。

【００１２】

第８に、第７の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００１３】

第９に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の可変の属性情報の有効性がそれ自身で証明されるので、匿名性が確保される。

【００１４】

第１０に、第９の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００１５】

第１１に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示制御情報に署名がされているので、発行者が規定した表示が保証される。

【００１６】

第１２に、第１１の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００１７】

第１３に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報の識別情報とを備えた電子情報を保存管理する手段を電子財布が備えたものである。表示制御情報の識別情報に署名がされているので、発行者が規定した表示が保証される。

【００１８】

第１４に、第１３の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００１９】

第１５に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示リソースの識別情報に署名がされているので、発行者が規定したイメージが保証される。

【００２０】

第１６に、第１５の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００２１】

第１７に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示制御情報の識別情報および表示リソースの識別情報に署名がされているので、発行者が規定した表示が保証される。

【００２２】

第１８に、第１７の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００２３】

第１９に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報ハンドラの認証鍵によって、電子情報ハンドラを認証

することができ、安全性が向上する。

【００２４】

第２０に、第１９の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００２５】

第２１に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報と表示リソースの識別情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を電子財布に備えたものである。
電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００２６】

第２２に、第２１の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００２７】

第２３に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及びサービス制御情報とを備えた電子情報を保存管理する手段を電子財布を備えたものである。サービス制御情報を変更することにより、各種の電子情報を規定することが出来る。

【００２８】

第２４に、第２３の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００２９】

第２５に、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示

制御情報の識別情報と表示リソースの識別情報と電子情報ハンドラの認証鍵及びサービス制御情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。サービス制御情報を変更することにより、各種の電子情報を規定することが出来る。

【００３０】

第２６に、第２５の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００３１】

第２７に、サービス制御情報が、少なくとも一つ以上のサービス制御モジュール情報の組合せにしたものである。サービス制御モジュール情報の組合せを変更することにより、各種の電子情報を規定することが出来る。

【００３２】

第２８に、電子情報の電子情報オブジェクトが、決済処理時に交換する各メッセージに、サービス制御情報に基づく決済データを重畳するようにしたものある。決済処理時に交換するメッセージ数を変えること無く、効率的な決済が可能となる。

【００３３】

第２９に、電子情報の電子情報オブジェクトが、決済処理時に交換する各メッセージに、サービス制御モジュール情報の組合せに基づく決済データを重畳するようにしたものである。決済処理時に交換するメッセージ数を変えること無く、効率的な決済が可能となる。

【００３４】

第３０に、電子情報の電子情報オブジェクトが、決済データを重畳するメッセージが、電子情報から電子情報ハンドラに決済処理を申し出るメッセージと、電子情報ハンドラから電子情報に属性値の変更を命令するメッセージと、電子情報から電子情報ハンドラに属性値の変更結果を示すメッセージと、電子情報ハンドラから電子情報への領収書に相当するメッセージであるようにしたものである。各種の電子情報における決済処理を、効率的に行うことが出来る。

【００３５】

第３１に、電子情報の表示手段を備えるようにしたものであり、電子情報の内容を確認することが出来、ユーザの利便性が向上する。

【００３６】

第３２に、電子情報から表示情報を生成する手段を備えるものであり、内容が変化した電子情報の内容を確認することが出来、ユーザの利便性が向上する。

【００３７】

第３３に、請求項１から請求項３２に記載の電子財布の処理プログラムを、電子計算機が読み取り可能な形式で記録したものであり、これにより、プログラムを、持ち運び可能な形態で、流通させることができる。

【００３８】

【発明の実施の形態】

以下、本発明の実施の形態について、図１から図２１を用いて説明する。なお、本発明はこれらの実施の形態に何ら限定されるものではなく、その趣旨を逸脱しない範囲において、種々なる態様で実施し得る。本発明の具体的な実施形態の一つであるモバイル・エレクトロニックコマース・システムは、個人消費者が、ネットワークを介して、各種のチケットや、プリペイドカードを電子情報として購入し、チケットの改札や、一般の小売販売店で商品を購入の際に、係員に対してチケットを提示したり、店員との間で、直接、現金やレシートを受け渡したりすることなく、全て、無線通信によって、チケットの改札、商品やサービスの売買決済を行なうシステムである。

【００３９】

以下では、本システムをモバイル・エレクトロニックコマース・システムと呼び、本システムで扱われる電子化されたチケットやプリペイドカードを電子バリュー、本システムによって提供される各種のサービスを、総称して、モバイル・エレクトロニックコマース・サービスと呼ぶこととする。このモバイル・エレクトロニックコマース・システムは、図１のシステム構成図に示すように、２系統の双方向無線通信機能とブラウザ機能と電子財布機能とを持つモバイルユーザ端末１０１と、双方向の通信機能とブラウザ機能と電子財布機能とを持つユーザ端

末１０７と、電子バリューの改札決済処理を行なうサービス端末１０５と、オンライン上で電子バリューの改札決済処理を行なうサービスサーバ１０６と、銀行、クレジットサービス会社または決済処理会社における口座決済処理を行なう決済処理サーバ１０４と、オンライン上で電子バリューに関する情報提供および電子バリューの販売を行う情報提供サーバ１０２と、電子バリューを生成・発行する電子バリュー発行サーバ１０３とを備え、これらはインターネット１００によって結ばれている。サービスサーバ１０６と決済処理サーバ１０４と情報提供サーバ１０２と電子バリュー発行サーバ１０３とは、それぞれ、１台もしくは複数台のコンピュータによって構成されるシステムである。

【００４０】

モバイルユーザ端末１０１は、赤外線通信とデジタル無線通信との２系統の双方向無線通信機能と、ブラウザ機能と電子財布機能とを持つ携帯無線電話端末である。また、サービス端末１０５は、赤外線通信とデジタル無線通信との２系統の双方向無線通信機能を持ち、用途に応じて据置タイプや携帯タイプがある。なお、図１において、１０８と１１３は、モバイルユーザ端末１０１とサービス端末１０５が、それぞれ、インターネット１００にアクセスしている際に行うデジタル無線通信の伝送路を示し、１０９は、モバイルユーザ端末１０１がサービス端末１０５と行う赤外線通信の伝送路を示し、１１０、１１１、１１２、１１４、１１５は、それぞれ、サービス提供サーバ１０２、電子バリュー発行サーバ１０３、決済処理サーバ１０４、サービスサーバ１０６、ユーザ端末１０７がインターネット１００に接続するデジタル通信回線を示している。

【００４１】

モバイル・エレクトロニックコマース・サービスの通常の運用形態としては、次のような形態を想定している。決済処理サーバ１０４は、銀行またはクレジットカード会社または決済処理会社に設置され、情報提供サーバ１０２は、イベント会社、チケット発行会社、小売販売会社またはプリペイドカード発行会社に、情報提供サーバ１０２は、オンライン上で電子バリューに関する情報の提供および電子バリューの販売を行う事業会社にそれぞれ設置される。また、サービス端末１０５は、据置タイプの場合には、映画館やイベント会場等の入口、小売販売

店のレジカウンタに設置され、携帯タイプの場合には、売場販売員や、集金担当者が携帯し、サービスサーバ１０６は、オンラインショップやインターネット放送など電子バリューに応じたサービスを提供する会社に設置される。モバイルユーザ端末１０１は、消費者が持ち歩き、ユーザ端末１０７は、消費者が自宅に設置する。電子バリュー発行サーバ１０３は、モバイル・エレクトロニックコマース・サービスを提供する会社に設置される。さらに、モバイル・エレクトロニックコマース・システムを構成する各機器、および、各システムの所有者間の社会的な関係として、次のような関係を前提としている。

【００４２】

モバイルユーザ端末１０１の所有する消費者は、銀行またはクレジットカード会社との間で、口座決済サービスの契約を、モバイル・エレクトロニックコマース・サービスを提供する会社との間では、モバイル・エレクトロニックコマース・サービスの会員契約を結んでいる。サービス端末１０５の所有者とサービスサーバ１０６の所有者は、モバイル・エレクトロニックコマース・サービスの提供者との間で、モバイル・エレクトロニックコマース・サービスの加盟店契約を結んでいる。但し、サービス端末１０５の所有者またはサービスサーバ１０６の所有者が、モバイル・エレクトロニックコマース・サービスの提供者と、同一の事業者であっても良い。情報提供サーバ１０６の所有者は、モバイル・エレクトロニックコマース・サービスの提供者との間で、情報提供サーバ１０６からの要求に応じて、電子バリュー発行サーバ１０３が電子バリューを発行する契約を結んでいる。但し、情報提供サーバ１０６の所有者が、モバイル・エレクトロニックコマース・サービスの提供者と、同一の事業者であっても良い。

【００４３】

以下では、本システムの説明を簡単にするために、モバイルユーザ端末１０１の所有する消費者をユーザ(User)、サービス端末１０５またはサービスサーバ１０６を所有し、商品やサービスを提供・販売する事業者をマーチャント(Merchant)、電子バリュー発行サーバ１０３を所有しモバイル・エレクトロニックコマース・サービスを提供する会社をサービス提供者(Service Provider)、決済処理サーバ１０４を所有し口座決済処理を行なう銀行、クレジットカード会社または決

済処理会社を決済処理機関(Transaction Processor)、情報提供サーバ１０２を所有し、オンライン上で電子バリューに関する情報提供および電子バリューの販売を行う事業者を電子バリュー販売者(Electronic Value seller)呼ぶこととする。本システムによって提供されるモバイル・エレクトロニックコマース・サービスは、ネットワークを介したチケットやプリペイドカードの売買と、それに伴うそれらの配送と、それらチケットやプリペイドカードの使用を、全て電子的に行なうサービスである。具体的には、ユーザがモバイルユーザ端末１０１を用いて、インターネットを介して、情報提供サーバ１０２に電子バリューの購入オーダーをし、電子バリュー発行サーバ１０３から、情報提供サーバ１０の電子バリュー発行要求に基づいて電子バリュー発行サーバ１０３が生成した電子バリューを受信して、それをモバイルユーザ端末１０１に蓄積して管理し、電子バリューを使用する際には、サービス端末１０５またはサービスサーバ１０６とのデータ通信によって、モバイルユーザ端末に蓄積されている電子バリューを提示し、電子バリューの改札決済処理情報を交換して、電子バリューの改札決済処理を行い、マーチャントが提供するサービスまたは商品の提供を行うものである。また、この時の電子バリューの売買に伴う決済処理は、情報提供サーバ１０と決済処理サーバ１４との間で行われる。モバイル・エレクトロニックコマース・サービスの詳細については、後で詳しく説明する。

【００４４】

モバイル・エレクトロニックコマース・サービスにおいて、本システムの各機器間で行われるデータ通信は、次に示す伝送路または通信回線を用いて行われる。まず、モバイルユーザ端末１０１は、伝送路１０８とインターネット１００とデジタル通信回線１１０とを介して情報提供サーバ１０２とデジタル通信を行い、伝送路１０８とインターネット１００とデジタル通信回線１１１とを介して電子バリュー発行サーバ１０３とデジタル通信を行い、伝送路１０８とインターネット１００とデジタル通信回線１１１とを介してサービスサーバ１０６とデジタル通信を行い、伝送路１０９を介してサービス端末１０５と赤外線通信を行う。また、モバイルユーザ端末１０１と電子バリュー発行サーバ１０３との通信、モバイルユーザ端末１０１とサービス端末１０５との通信、モバイルユーザ端末１

０１とサービスサーバ１０６との通信では、交換される情報を、全て、暗号化して通信する。暗号化には、秘密鍵方式の暗号処理と公開鍵方式の暗号処理とを組合わせて、情報を電子封書化して通信する。

【００４５】

次に、本システムを構成する各構成要素について説明する。まず、サービス端末１０５について説明する。図６は、サービス端末１０５のブロック構成図である。図６において、サービス端末１０５は、コンピュータ６００と無線通信モデム６０１と赤外線通信アダプタ６０２によって構成される。サービス端末１０５には、デジタル無線通信と赤外線通信の２系統の通信機能があり、デジタル無線通信機能によってインターネットアクセスを行い、赤外線通信機能によってモバイルユーザ端末との電子バリューの改札決済処理を行う。コンピュータ６００には、マーチャントアプリケーションが搭載されており、このマーチャントアプリケーションに基づいて、コンピュータ６００が無線通信モデム６０１と赤外線通信アダプタ６０２を制御して、電子バリューの改札決済処理を行う。同様に、サービスサーバ１０６にも、マーチャントアプリケーションが搭載されており、サービスサーバ１０６は、このマーチャントアプリケーションに基づいて、電子バリューの改札決済処理を行う。改札決済処理におけるサービス端末１０５とサービスサーバ１０６の詳細な動作とについては、後で詳しく説明する。

【００４６】

次に、ユーザ端末１０７について説明する。図７は、ユーザ端末１０７のブロック構成図である。図７において、ユーザ端末１０７は、コンピュータ７００とスマートカードリーダライタ７０１と通信モデム７０２によって構成される。ユーザ端末１０７には、ブラウザアプリケーションプログラムと電子財布アプリケーションプログラムが搭載されており、インターネットへのアクセスは通信アダプタ７０２によって行う。ユーザ端末１０７は、スマートカードリーダライタ７０１に、モバイルユーザ端末１０１のスマートカードを挿入することにより、サービス端末１０５との改札決済処理を除いて、モバイルユーザ端末１０１と同じ機能を持つ。

【００４７】

次に、モバイルユーザ端末１０１について説明する。図２（ａ）、図２（ｂ）は、それぞれ、モバイルユーザ端末１０１の前面側及び背面側の外観図である。図２（ａ）において、２１１は、サービス端末１０５と赤外線通信を行なう赤外線通信ポート（赤外線通信モジュール）、２１０は、デジタル無線通信の電波を受発信するアンテナ、２０９は、レシーバスピーカ、２００は、１２０×１６０画素表示のカラー液晶ディスプレ（ＬＣＤ）、２０３は、通話スイッチ、２０２は、通話の終了スイッチと電源スイッチを兼ねた終了／電源スイッチ、２０４は、ナビゲーションスイッチ、２０５と２０６はファンクションスイッチ、２０１は、テンキースイッチ、２０７は、マイクである。さらに、図２（ｂ）において、２１２は、スマートカードスロット（スマートカードリーダライタ）である。

【００４８】

モバイルユーザ端末１０１には、デジタル無線通信と赤外線通信の２系統の通信機能があり、デジタル無線通信機能によって音声通話とインターネットアクセス、及びサービスサーバとの電子バリューの改札決済処理を行い、赤外線通信機能によってサービス端末との電子バリューの改札決済処理を行う。さらに、モバイルユーザ端末１０１には、ブラウザ機能と電子財布機能があり、ブラウザ機能によってインターネットとモバイルユーザ端末のローカルデータのブラウジングを行い、電子財布機能によって電子バリューの管理、及び改札決済処理を行う。図３は、モバイルユーザ端末１０１のブロック構成図である。図３において、モバイルユーザ端末１０１は、ＦｅＲＡＭ(Ferroelectronic Random Access Memory)３０１に格納されたプログラムにしたがって、ＦｅＲＡＭ３０１に格納されたデータの処理と送受信データの処理、並びにバス３０６を介して他の構成要素の制御を行なうＣＰＵ(Central Processing Unit) ３００と、ＬＣＤ１００と、赤外線通信モジュール１１１と、スマートカードリーダライタ１１２と、テンキースイッチ１０１、終了／電源スイッチ１０２、通話スイッチ１０３、ナビゲーションスイッチ１０４、及びファンクションスイッチ１０５，１０６と、スイッチ操作を検出するキー制御部３０２と、スピーカ３０３とレシーバ１０９をドライブしマイク１０７から入力するアナログ音声信号をデジタル処理する音声処理部３０４と、アンテナ１１０を介して行う無線データ通信及び無線音声通信を制御

する無線通信部３０５と、スマートカード３０７とによって構成される。

【００４９】

スマートカード３０７は、ＣＰＵと不揮発性メモリを内蔵し、不揮発性メモリには、ユーザのＵＰＴ(Universal Personal Telecommunication)番号（電話番号）と、モバイル・エレクトロニックコマース・サービスにおけるユーザＩＤと、公開鍵暗号方式のユーザ秘密鍵と、それに対応するユーザ証明書、並びに、サービス提供者証明書（サービス提供者のデジタル証明書）と、ユーザが購入した電子バリューと、電子バリューの購入及び改札決済処理の領収書が格納される。ＦｅＲＡＭ３０１には、ＯＳ（Operating System）と電話の他に、ブラウザと電子財布の２つのアプリケーションプログラムが格納されており、ＣＰＵ３００は、これらのアプリケーションを同時に実行する。

【００５０】

図４は、ＣＰＵ３００が実行するアプリケーション（ブラウザと電子財布）と、モバイルユーザ端末１０１の他の構成要素と、他の機器との関係を示す模式図である。図４において、ＣＰＵ３００は、ブラウザ４０１と電子財布４００の２つのプロセスを実行する。ブラウザ４０１は、キー制御部３０２から送られるユーザ操作情報　（スイッチ操作）に基づいて、無線通信部３０５を用いて、情報提供サーバ１０３とインターネット１００を介して通信し、情報提供サーバ１０３から受信したデータを解釈して、ＬＣＤ２００に表示する。この時、情報提供サーバ１０３から受信するデータは、特定のマークアップ記述言語に基づいて記述されており、ブラウザ４０１は、このマークアップ記述言語を解釈して画像データを生成し、ＬＣＤ２００に表示する。また同様に、ブラウザ４０１は、ＦｅＲＡＭ３０１に格納されたファイルや、電子財布４００から受信したデータを解釈し、ＬＣＤ２００に表示する。この時、ＦｅＲＡＭ３０１に格納されたファイル、及び電子財布４００から受信したデータは、特定のマークアップ記述言語に基づいて記述されている。例えば、図５（ａ）は、電源をオンした時にＬＣＤ２００に表示されるマイメニュー画面を示している。終了／電源スイッチ２０２によって電源をオンすると、ブラウザ４０１は、まず、ＦｅＲＡＭ３０１に格納されたマイメニューファイルを読出し、図５（ａ）に示す画面を表示する。マイメ

ニューファイルは、モバイルユーザ端末１０１の操作メニューであり、特定のマークアップ記述言語に基づいて記述されている。

【００５１】

ここで例えば、”１ Internet”を選択すると、ブラウザ４０１は、インターネットにアクセスし、”１ Internet”にリンクされた図５（ｂ）に示すインターネットメニュー画面を表示する。ユーザは、このインターネットメニュー画面からインターネット上のサイト、例えば情報提供サーバ１０２にアクセスをする。図５（ｃ）は、情報提供サーバ１０２にアクセスし、電子バリューをオーダーする場合の画面の一例を示している。また、”２ E-Wallet”を選択すると、ブラウザ４０１は、電子財布４００にアクセスし、電子財布４００から受信したデータに基づいて、図５（ｄ）に示すパスワードの入力を要求する画面を表示する。さらにこの画面でパスワードを入力すると、ブラウザ４０１は、入力されたパスワードを電子財布４００に送信し、パスワードが正しい場合、電子財布４００からブラウザ４０１に、電子財布４００で管理されている電子バリューの一覧を示すデータが送信され、ブラウザ４０１は、図５（ｅ）に示す画面を表示する。パスワードが間違っている場合には、エラー画面が表示される。さらに、”７ Soccer ２００X Japa”を選択すると、電子財布４００からブラウザ４０１に、選択された電子バリューの内容を示すデータが送信され、ブラウザ４０１は、図５（ｆ）に示す画面を表示する。以上において、電子財布４００からブラウザ４０１に送信されるデータは、特定のマークアップ記述言語に基づいて記述されている。

【００５２】

図５（ａ）～（ｆ）に示すように、ブラウザ４０１がＬＣＤ２００に表示する画面は、受信したデータを表示するコンテンツ表示領域５００と、画面上部の状態表示領域５０２と、画面下部のメニュー表示領域５０２の３つの領域に分けられる。状態表示領域５０２には、現在、どこと通信しているか、及び通信がセキュアか否かが示される。例えば、図５（ｃ）の場合には、表示されている画面がインターネットをアクセスしたもので、その通信がセキュアーな通信で盗聴されないことを示している。また、図５（ｅ）の場合には、表示されている画面が電子財布４００をアクセスしたもので、ブラウザ４０１と電子財布４００間の通信

がセキュアーな通信で盗聴されないことを示している。メニュー表示領域５０２は、表示中の画面において、ファンクションスイッチ２０５、２０６に割り当てられたファンクションを示す領域である。例えば、図５（ａ）の場合には、ファンクションスイッチ２０５に”ＯＫ”つまり「選択」を意味するファンクションが割り当てられ、ファンクションスイッチ２０６に"back"つまり「戻る」を意味するファンクションが割り当てられる。

【００５３】

一方、電子財布４００は、ブラウザ４０１からの要求に応じて、電子バリュー発行サーバ１０３からの電子バリューの受信と、スマートカード３０７に格納された電子バリューの管理、及びサービス端末１０５またはサービスサーバ１０６との改札決済処理を行う。例えば、図５（ａ）のマイメニュー画面で、ユーザが”２ E-Wallet"を選択した場合、”２ E-Wallet"には、"wallet:///index"というＵＲＩ（Uniform Resource Identifier）がリンクされており、ブラウザ４０１は電子財布４００に電子財布内のインテックス情報つまり電子財布４００で管理されている電子バリューの一覧を要求する。それに対し、電子財布４００は、特定のマークアップ記述言語で記述されたパスワード入力画面データをブラウザ４０１に返し、次にブラウザからユーザが入力したパスワードが送信されると、スマートカードリーダライタ２１２を介してスマートカード３０７にアクセスし、スマートカード３０７に登録されたパスワードと照合してパスワードが正しい場合に、つまりユーザが認証された場合に、特定のマークアップ記述言語で記述されたスマートカード３０７に格納されている電子バリューの一覧を示すデータをブラウザ４０１に返す。

【００５４】

さらに、図５（ｅ）の電子バリューの一覧画面で、ユーザが”７ Soccer ２００X Japa”を選択した場合、”７ Soccer ２００X Japa”には、"wallet:///Evalue/ev００００００３３"というＵＲＩがリンクされており、ブラウザ４０１は電子財布４００に"ev ００００００３３”という識別子で管理されている電子バリューを要求する。それに対し、電子財布４００は、スマートカードリーダライタ２１２を介してスマートカード３０７にアクセスし、スマートカード３０７の

不揮発性メモリに"ev ００００００３３"という識別子で格納管理されている電子バリューデータから、電子バリューオブジェクトを生成し、さらに、生成した電子バリューオブジェクトに電子バリューの内容を示すデータを要求し、電子バリューオブジェクトが生成した電子バリューの内容を示すデータを、ブラウザ４０１に返す。この時、電子バリューオブジェクトが生成する電子バリューの内容を示すデータは、特定のマークアップ記述言語に基づいて記述されている。

【００５５】

また例えば、電子バリューの購入の場合には、電子財布４００は、ブラウザ４０１からの電子バリューの受信要求に基づいて、電子バリュー発行サーバ１０３からの電子バリューを受信する。このブラウザからの電子バリューの受信要求には、電子バリュー発行サーバ１０３のＵＲＩ（http://www.evalue.com）と、受信する電子バリューを示すセッション番号が含まれ、この電子バリュー発行サーバ１０３のＵＲＩとセッション番号は、ブラウザ４０１の情報提供サーバ１０２への電子バリューの購入オーダーに対して情報提供サーバ１０２からブラウザ４０１に送信される電子バリューの受信を指示するデータの中に含まれている。ブラウザ４０１から電子バリューの受信を要求され電子財布４００は、無線通信部３０５を介して電子バリュー発行サーバ１０２にアクセスし、スマートカード３０７に格納されているユーザ秘密鍵とユーザ証明書とサービス提供者証明書を用いて、電子バリュー発行サーバ１０２との間で暗号化通信セッションを確立して、電子バリュー発行サーバ１０２に電子バリューの発行を要求し、電子バリュー発行サーバ１０２から電子バリューを含むデータを受信する。この時、電子財布から電子バリュー発行サーバに送信される電子バリューの発行要求には、電子財布が受信する電子バリューを示すセッション番号が含まれる。電子バリューを含むデータを受信した電子財布４００は、受信したデータから電子バリューオブジェクトを生成し、さらに、生成した電子バリューオブジェクトに電子バリューデータの生成を要求し、電子バリューオブジェクトが生成した電子バリューデータをスマートカード３０７に格納して、電子バリューを電子財布に登録する。ここで電子バリューデータとは、電子バリューオブジェクトを特定のフォーマットのシリアルデータに変換したものであり、また、そのシリアルデータに、さらに暗

号化を施したものであっても良い。

【００５６】

また、電子バリューの改札決済処理の場合には、電子財布４００は、ブラウザ４０１からの電子バリューの改札決済処理要求に基づいて、サービス端末１０５またはサービスサーバ１０６との間で改札決済処理を行う。ブラウザ４０１からの改札決済処理要求に対し、ブラウザ４０１がサービスサーバ１０６と通信中の場合には、電子財布４００は無線通信部５a-０５を介してサービスサーバ１０６と改札決済処理を行い、ブラウザ４０１がサービスサーバ１０６と通信していない場合には、電子財布４００は赤外線通信モジュール２a-１１を介してサービス端末１０５と改札決済処理を行う。電子バリューの改札決済処理については後で詳しく説明する。次に、スマートカード３０７に格納される電子バリュー（電子バリューデータ）のデータ構造について説明する。図８は、電子バリューのデータ構造を示す模式図である。図８において、一つの電子バリューは、バリュー属性記述部８００、サービス制御部８０３、セキュリティ情報部８０４、表示制御部８０５、表示リソース部８０６の５つの部分から構成される。

【００５７】

バリュー属性記述部８００は、電子バリューのタイプ、コード番号、ＩＤ番号、名称など、各種属性を規定する部分であり、バリュー属性記述部８００は、さらに、改札決済処理により値が変化しない固定属性を示すプレゼンテーションカード８０１と、改札決済処理により値が変化する可変属性８０２に分けられる。サービス制御部８０３は、電子バリューが改札決済処理で行う処理の内容を規定する部分であり、セキュリティ情報部８０４は、電子バリューが持つ暗号鍵等の機密情報を規定する部分、表示制御部８０５は、電子バリューの表示を規定する部分、表示リソース部８０６は、電子バリューの表示及びサウンド効果に用いるイメージデータや音声データ等を規定する部分である。また、電子バリューのデータ構造は、特定のマークアップ記述言語に基づいており、スマートカード３０７には、それをさらにエンコードしたものが格納される。

【００５８】

図１２は、特定のマークアップ記述言語で記述された電子バリューの一例を、

一部省略して示しており、この場合、この電子バリューは、電子財布４００に”ev ００００００３３”という識別子で管理されている。プレゼンテーションカード８０１は、サービス提供者（http://www.evalue.com）によりデジタル署名されており、可変属性８０２は、この電子バリューの秘密鍵（ev Private Key）によって、つまり、この電子バリュー自身によってデジタル署名されている。また、サービス制御部８０３とセキュリティ情報部８０４と表示制御部８０５と表示リソース部８０６は、サービス提供者（http://www.evalue.com）によりデジタル署名されている。これらのデジタル署名は、電子バリューオブジェクトが生成される度に検証される為、これらの部分に不正な改竄をすることは難しい。ただし、表示制御部８０５と表示リソース部８０６は、そのＵＲＩのみ規定されており、表示制御部の実体は、１２０１の部分で、表示リソース部の実体は、１２０２の部分で、それぞれ個別に規定される。または、サービス提供者（http://www.evalue.com）についても、１２００の部分で規定される。

【００５９】

図１３は、図１２に示した電子バリューのプレゼンテーションカード８０１と可変属性８０２ を省略無しに示したものである。図１３によれば、この電子バリューには、固定属性として、電子バリューのタイプ(evType)がチケット(ticket)で、コード番号(evCode)が、

”０００３０００００００２０１”

また、ＩＤ番号(evID)が、

”１０００００００００００００００００００００００００００００１”

チケットのタイトル(TITLE)が、

”Soccer２００X Japan vs Brazil”

席番号(SEAT__NUM)が、

”SS-A-２８”

等の属性があり、また可変属性として、

有効性フラグ(VALIDITY)が”１”（つまり有効）で、

使用済フラグ(USED)が”０”（つまり未使用）で、

回数券枚数(NUMBER)が”１”（つまり１回使い切りのチケット）

といった属性を持っている。

【００６０】

図１４は、図１２に示した電子バリューのサービス制御部８０３とセキュリティ情報部８０４を省略無しに示したものである。図１４によれば、この電子バリューには、チケットモジュール(ticket)と属性検証モジュール(verify__prop)とメッセージ設定モジュール(set__message)の３つのサービス制御モジュールが規定されている。ここで、サービス制御モジュールとは、改札決済処理で行う処理を、小さな処理モジュールに部品化したものである。改札決済処理では、サービス制御部８０３に規定されたサービス制御モジュールがそれぞれ実行される。つまり、サービス制御部８０３に規定するサービス制御モジュールの組合わせを変えることによって、各種の改札決済処理を規定することが出来る。例えば、この電子バリューの場合、チケットモジュールは、チケットの基本機能をモジュール化したものであり、改札決済処理によって、チケットの回数券枚数($NUMBER)を”１”デクリメントし、有効期間の開始日時($START__VALID)と終了日時($END__VALID)をそれぞれ設定し、使用済フラグ($USED)を”１”（つまり使用済）に、有効性フラグ($VALIDITY)を有効期間に応じて設定し、電子バリューを使用した回数、つまり改札決済処理の回数を示す使用シリアル番号($USE__SERIAL)を”１”インクリメントする。属性検証モジュールは、指定された電子バリューの属性を検証するモジュールであり、この場合、改札決済処理によって席番号($SEAT__NUM)が検証される。

【００６１】

メッセージ設定モジュールは、メッセージ（文字列）を設定するモジュールであり、改札決済処理によって、可変属性の１つであるメッセージ２($MESSAGE__２）に、サービス端末１０５（または、サービスサーバ１０６）に設定されたメッセージが設定される。以上の処理が、１回の改札決済処理の中で、同時に行われる。また、セキュリティ情報部８０４には、この電子バリュー固有の鍵である公開鍵暗号方式の電子バリュー秘密鍵(evPrivateKey)と、それに対応する電子バリュー証明書(evCertificate)、並びに、電子バリューのコード番号毎に固有の鍵である共通鍵方式の電子バリュー認証鍵(evAuthKey)と電子バリューハンド

ラ認証鍵(evhandlerAuthKey)等が規定されている。ここで、電子バリューハンドラとは、この電子バリューと改札決済処理を行うサービス端末１０５またはサービスサーバ１０６に、予め設定されている改札決済処理のための情報である。サービス端末１０５またはサービスサーバ１０６では、改札決済処理時に、この情報から電子バリューハンドラオブジェクトが生成され、実質的に、電子バリューオブジェクトと電子バリューハンドラオブジェクトとの間で改札決済処理が行われる。電子バリューハンドラについては、後で詳しく説明する。

【００６２】

図１５は、図１２に示した電子バリューの表示制御部８０５を省略無しに示したものである。図１５によれば、この電子バリューには、"Main"と"Detail"の２つの画面情報が規定されている。表示制御部８０５には、マークアップ記述言語による表示画面のテンプレートが規定されている。この電子バリューの電子バリューオブジェクトは、<evP>と</evP>に挟まれた部分をプレゼンテーションカード８０１で規定されている属性の値に、<evV>と</evV>に挟まれた部分を可変属性８０２で規定されている属性の値に、それぞれ置きかえることによって、電子バリューの内容を示すデータを生成する。例えば、図５（ｅ）の電子バリューの一覧画面で、ユーザが" 7 Soccer ２００X Japa" を選択した場合には、電子バリューオブジェクトは、図１７に示す"Main"の画面情報を生成し、ブラウザ４０１によって、ＬＣＤ２００には、図５（ｆ）に示す画面が表示される。

【００６３】

図１６は、図１２に示した電子バリューの表示リソース部８０６を省略無しに示したものである。図１６によれば、この電子バリューには、"MAIN__IMG" と"MAP"というラベルが付けられた２つのイメージデータと、"Greet"というラベルが付けられた１つの音声データが規定されている。例えば、図１７に示した"Main"の画面情報の場合、"<IMG SRC="wallet:///evResource label=MAIN__IMG" >"の部分は、電子財布４００に存在する電子バリューオブジェクトの表示リソース部の中のラベルが"MAIN__IMG"のイメージの表示を規定している記述であり、図１６に示したリソースデータの内、"MAIN__IMG"というラベルが付いたイメージデータが、ブラウザ４０１に送られ、図５（ｆ）に示すような画面が表示され

る。このように、一つの電子バリューが持つ各種の属性、改札決済処理で行う処理の内容、及び電子バリューの表示は、このようなマークアップ記述言語に基づいて規定される。

【００６４】

なお、電子バリューの表示制御部の実体１２０１と表示リソース部の実体１２０２は、スマートカード３０７に格納せずに、ＦｅＲＡＭ３０１に格納しするようにしても良い。この場合、スマートカード３０７に、より多くの電子バリューを格納することが出来るというメリットがある。ただしこの場合、ユーザ端末１０７のスマートカードリーダライタ７０１にスマートカード３０７を挿入して、コンピュータ７００の画面に電子バリューの内容を表示する際、表示制御部の実体１２０１と表示リソース部の実体１２０２が必要になるが、表示制御部８０５と表示リソース部８０６に規定されているそれらの実体のＵＲＩを基に、インターネット１００を介して表示制御部の実体１２０１と表示リソース部の実体１２０２をダウンロードすることにより、電子バリューの内容を表示することが出来る。

【００６５】

次に、電子バリューハンドラについて説明する。電子バリューハンドラは、電子バリューのコード番号に対応して存在し、サービス提供者によって、予め、その電子バリューを取り扱うマーチャントのサービス端末１０５及びサービスサーバ１０６に対して、インターネット１００を介して配布されている。図９は、電子バリューハンドラのデータ構造を示す模式図である。図９において、一つの電子バリューハンドラは、バリュー属性記述部９００、サービス制御部９０３、セキュリティ情報部９０４とマーチャントオプション９０５の４つの部分から構成される。バリュー属性記述部９００は、取り扱う電子バリューのタイプ、コード番号、ＩＤ番号、名称など、各種属性を規定する部分でり、サービス制御部９０３は、電子バリューとの改札決済処理で行う処理の内容を規定する部分であり、セキュリティ情報部９０４は、電子バリューハンドラが持つ暗号鍵等の機密情報を規定する部分、マーチャントオプション９０５は、マーチャント独自の追加設定を規定する部分である。電子バリューハンドラもまた、そのデータ構造は、特

定のマークアップ記述言語に基づいており、サービス端末１０５またはサービスサーバ１０６には、それをさらにエンコードしたものが格納される。

【００６６】

図１８は、図１２に示した電子バリューに対応する電子バリューハンドラのマークアップ記述言語による記述を一部省略して示しており、この場合、この電子バリューハンドラは、電子マーチャントに"ev ０００００００１"という識別子で管理されている。電子バリューハンドラを構成するデータの内、バリュー属性記述部９００とサービス制御部９０３とセキュリティ情報部９０４がサービス提供者から配布されたものであり、マーチャントオプション９０５は、マーチャントがマーチャントアプリケーションによって追加設定したものである。したがって、バリュー属性記述部９００とサービス制御部９０３とセキュリティ情報部９０４の部分にのみ、サービス提供者（http://www.evalue.com）によるデジタル署名が施されている。このデジタル署名は、電子バリューハンドラオブジェクトが生成される度に検証される為、これらの部分に不正な改竄をすることは難しい。

【００６７】

図１８のバリュー属性記述部９００によれば、取り扱う電子バリューは、電子バリューのタイプ(evType)がチケット(ticket)で、コード番号(evCode)が"００００３０００００００２０１"、チケットのタイトル(TITLE)が"Soccer２００X Japan vs Brazil"といった属性を持っている。ただし、席番号(SEAT__NUM)とメッセージ２(MESSAGE__２）に関しては規定されておらず、それぞれには、電子バリューハンドラの所有者（マーチャント）による設定を許可するpermission="public"という要素が付加されている。これにより、マーチャントによるマーチャントオプション９０５の追加が可能になり、例えば、図１８のマーチャントオプション９０５では、席番号($SEAT__NUM)に"SS-*-*"が、メッセージ２($MESSAGE__２）に" Special News available: http://www.yis.co.jp/news/２００２０６３０"がそれぞれ設定されている。

【００６８】

図１８のサービス制御部９０３には、電子バリューのチケットモジュール(tic

ket)と属性検証モジュール(verify__prop)とメッセージ設定モジュール(set__message)に対応するサービスモジュールが規定されている。マークアップ記述言語による記述は電子バリューと同じであるが、それぞれ、マーチャント側の処理を行うサービスモジュールが実行される。例えば、属性検証モジュールの場合には、マーチャントオプション９０５の設定にしたがって、席番号($SEAT__NUM) が、"SS-*-*"と照合される。この時、'*'は任意の文字列を意味し、SS席のチケットのみ、改札決済処理が可能となる。また、メッセージ設定モジュールの場合には、マーチャントオプション９０５の設定にしたがって、改札決済処理により、電子バリュー側のメッセージ２($MESSAGE__２）に" Special News available: http://www.yis.co.jp/news/ ２００２０６３０"というメッセージが設定される。

【００６９】

図１８のセキュリティ情報部９０４には、図１２に示した電子バリューのセキュリティ情報部８０４に規定されているものと同じ電子バリュー認証鍵(evAuthKey)と電子バリューハンドラ認証鍵(evhandlerAuthKey)が規定されている。電子バリューと電子バリューハンドラは、改札決済処理の際、この電子バリュー認証鍵(evAuthKey)と電子バリューハンドラ認証鍵(evhandlerAuthKey)を用いて相互認証を行う。

【００７０】

次に、モバイルユーザ端末１０１とサービス端末１０５間の改札決済処理について説明する。改札決済処理は、ユーザが使用する電子バリューをＬＣＤ２００に表示し、赤外線通信ポート（赤外線通信モジュール）をサービス端末１０５の赤外線通アダプタ６０２に向けて、改札決済処理の実行に割り付けられたファンクションスイッチを押すことによって開始する。例えば、図１７に示した"Main"の画面の場合、改札決済処理の実行に割り付けられたファンクションスイッチを押すことによって、<Go HREF="wallet:///evTransact"/>が実行され、電子財布４００上の電子バリューオブジェクトに改札決済処理が要求される。

【００７１】

図１０は、改札決済処理においてモバイルユーザ端末１０１とサービス端末１

０５間で交換されるメッセージを示している。まず、電子バリューオブジェクトから電子バリューの改札決済処理を申し出るメッセージ、プレゼンテーション（Presentation）１００３が送信される。それに対し、サービス端末１０５のマーチャントアプリケーションは、電子バリューに対応する電子バリューハンドラオブジェクトを生成し、生成された電子バリューハンドラオブジェクトから電子バリューに属性の値の変更を要求するメッセージ、インストラクション（Instruction）１００４が送信される。電子バリューオブジェクトは、インストラクション１００４に基づいて属性の値を変更し、その変更を証明するメッセージ、トランザクション（Transaction）１００５を電子バリューハンドラオブジェクトに送信する。電子バリューハンドラオブジェクトは、トランザクション１００５の内容を検証し、正しい場合に、トランザクション１００５の領収書に相当するレシート（Receipt）１００６を送信する。さらに、電子バリューオブジェクトは、レシート１００６の内容を検証し、正しい場合に、レシート１００６の受け取り確認（アクノレッジ）に相当するメッセージ、アクノレッジ（Acknowledge）１００７を電子バリューハンドラオブジェクトに送信し、属性の値が変更された電子バリューデータとレシートをスマートカードａ５－０７に保存して改札決済処理を終了する。改札決済処理の途中で、エラーが発生した場合には、相手側にエラーメッセージを送信して改札決済処理を中止する。

【００７２】

プレゼンテーション１００３は、図１１（ａ）に示すように、メッセージのヘッダ１１１０と、この改札決済処理を電子財布ａ６－００からみてユニークに示す要求番号１１１１と、電子バリューのプレゼンテーションカード１０１２（８０１）と、サービス制御モジュールによるサービス制御メッセージ１１１３に、電子バリュー秘密鍵による電子バリュー署名ａ１４－１４をし、さらに電子バリュー証明書１１１５を付加して、これを電子バリューハンドラ認証鍵で暗号化して、さらにメッセージのヘッダ１１１７と電子バリューのコード番号１１１８を付加したものである。サービス端末１０５のマーチャントアプリケーションは、プレゼンテーション１００３のコード番号１１１８に基づいて、電子バリューに対応する電子バリューハンドラオブジェクトを生成し、生成された電子バリュー

ハンドラオブジェクトは、まず、電子バリューハンドラ認証鍵によって暗号化されている部分１１１６を復号化し、電子バリュー証明書１１１５さらには電子バリュー署名ａ１４－１４を検証して、サービス制御メッセージ１１１３を検証する。プレゼンテーション１００３の検証結果が正しい場合に、電子バリューハンドラオブジェクトはインストラクション１００４を生成、送信する。

【００７３】

インストラクション１００４は、図１１（ｂ）に示すように、メッセージのヘッダ１１２０と、プレゼンテーション１００３に含まれていた要求番号１１２１（１１１１）と、この改札決済処理をマーチャントアプリケーションからみてユニークに示す決済番号１１１２と、サービス制御モジュールによるサービス制御メッセージ１１２３に、マーチャント秘密鍵によるマーチャント署名ａ１４－２４をし、さらにマーチャント証明書１８２５と、新たに生成したセッション鍵Ａ１１２６を付加して、これを電子バリュー認証鍵で暗号化して、さらにメッセージのヘッダ１１２８を付加したものである。電子バリューオブジェクトは、まず、電子バリュー認証鍵によって暗号化されている部分１１２７を復号化し、電子マーチャント証明書１１２５さらにはマーチャント署名ａ１４－２４を検証して、要求番号１１１１を照合し、サービス制御メッセージ１１１３を検証する。インストラクション１００４の検証結果が正しい場合、はじめて、電子バリューハンドラオブジェクトが正しい電子バリュー認証鍵と電子バリューハンドラ認証鍵とを持つ正当な電子バリューハンドラオブジェクトであと判定し、電子バリューオブジェクトは、インストラクション１００４に基づいて属性の値を変更し、トランザクション１００５を生成、送信する。トランザクション１００５は、図１１（ｃ）に示すように、メッセージのヘッダ１１３０と、要求番号１１３１と、インストラクション１００４に含まれていた決済番号１１３２（１１２２）と、トランザクション１００５の宛先に相当するマーチャントＩＤ１１３３と、サービス制御モジュールによるサービス制御メッセージ１１３４に、電子バリュー秘密鍵による電子バリュー署名ａ１４－３５をし、新たに生成したセッション鍵Ｂ１１３６を付加して、これをインストラクション１００４に含まれていたセッション鍵Ａ１１２６で暗号化して、さらにメッセージのヘッダ１１３８を付加した

ものである。

【００７４】

電子バリューハンドラオブジェクトは、まず、セッション鍵Ａ１１２６によって暗号化されている部分１１３７を復号化し、電子バリュー署名ａ１４－３５を検証して、要求番号１１１１及び決済番号１１３２を照合し、サービス制御メッセージ１１１３を検証する。トランザクション１００５の検証結果が正しい場合、はじめて、電子バリューオブジェクトが正しい電子バリュー認証鍵と電子バリューハンドラ認証鍵とを持つ正当な電子バリューオブジェクトであると判定し、電子バリューハンドラーオブジェクトは、トランザクション１００５の領収書に相当するレシート１００６を生成、送信する。

【００７５】

レシート１００６は、図１１（ｄ）に示すように、メッセージのヘッダ１１４０と、要求番号１１４１（１１３１）と、決済番号１１４２（１１３２）と、レシート１００６の宛先に相当する電子バリューＩＤ１１４３と、サービス制御モジュールによるサービス制御メッセージ１１４４と、領収書情報１１４５とに、マーチャント秘密鍵によるマーチャント署名ａ１４－４６をし、さらに、トランザクション１００５に含まれていたセッション鍵Ｂ１１３６で暗号化して、さらにメッセージのヘッダ１１４８を付加したものである。電子バリューオブジェクトは、まず、セッション鍵Ｂ１１３６によって暗号化されている部分１１４７を復号化し、マーチャント署名ａ１４－４６を検証して、要求番号１１１１及び決済番号１１３２を照合し、サービス制御メッセージ１１１３を検証する。レシート１００６の検証結果が正しい場合、電子バリューオブジェクトは、が正しい電子バリュー認証鍵と電子バリューハンドラ認証鍵とを持つ正当な電子バリューオブジェクトであと判定し、電子バリューハンドラーオブジェクトは、レシート１００６の受け取り確認に相当するアクノレッジ１００７を生成、送信する。

【００７６】

アクノレッジ１００７は、図１１（ｅ）に示すように、メッセージのヘッダ１１５０に、レシート１００６に対する電子バリュー秘密鍵による電子バリュー署名ａ１４－５１を付加したものである。電子バリューハンドラオブジェクトは、

電子バリュー署名ａ１４－５１を検証して、正しい場合に、復号化されたトランザクションとレシートを保存して改札決済処理を終了する。一方、アクノレッジ１００７を送信した電子バリューオブジェクトは、属性の値を変更した電子バリューデータと、復号化されたレシートをスマートカードａ５－０７に保存して改札決済処理を終了する。この際、電子バリューの可変属性８０２には、電子バリュー秘密鍵によって新たにデジタル署名が施される。

【００７７】

また、この改札決済処理において、プレゼンテーション１００３とインストラクション１００４とトランザクション１００５とレシート１００６の各メッセージに設定されるサービス制御メッセージによって、各電子バリューに固有の改札決済処理が行われる。サービス制御メッセージは、サービス制御モジュールによって設定され、相手側のサービス制御モジュールによって検証される。プレゼンテーション１００３とインストラクション１００４とトランザクション１００５とレシート１００６には、それぞれ、図１９（ａ）、（ｂ）、（ｃ）、（ｄ）に示すデータをエンコードしたものが、サービス制御メッセージとして設定される。例えば、図１９（ａ）の場合、電子バリューハンドラオブジェクト側のＩＤが”１”のサービス制御モジュール（チケットモジュール）に対しnumber= 1 start=”１９９９．０７．２３Ｔ００：００+０９００” end=”２００２．０６．３０Ｔ２３：５９+０９００” used__flag= 0 validity__flag= 1 serial=0、ＩＤが”２”のサービス制御モジュール（属性検証モジュール）に対しprop=SS-A-２８、ＩＤが”３”のサービス制御モジュール（メッセージ設定モジュール）に対しmsg=というように、現状の電子チケットの属性が提示され、電子バリューハンドラオブジェクトのそれぞれのサービス制御モジュールにおいて検証される。例えばこの時、電子バリューハンドラが図１８に示したもので、prop=S-A-２８であった場合には、照合エラーとなる。

【００７８】

図１９（ｂ）の場合、電子バリューオブジェクト側のＩＤが”１”のサービス制御モジュール（チケットモジュール）に対しnumber= 0 start=”２００２．０６．３０Ｔ１２：２５+０９００” end=”２００２．０６．３０Ｔ２３：５９+

０９００” used __flag= 1 validity__flag= 1 serial=1、ＩＤが” ３”のサービス制御モジュール（メッセージ設定モジュール）に対しmsg=”Special News available: http://www.yis.co.jp/news/２００２０６３０ ” というように、属性の変更命令が提示され、電子バリューオブジェクトのそれぞれのサービス制御モジュールにおいて属性が変更される。

【００７９】

図１９（ｃ）の場合、電子バリューハンドラオブジェクト側のＩＤが” １”のサービス制御モジュール（チケットモジュール）に対しnumber= ０ start=”２００２．０６．３０T １２：２５+ ０９００” end=” ２００２．０６．３０T ２３：５９+ ０９００” used__flag= 1 validity__flag= 1 serial=1、ＩＤが” ２”のサービス制御モジュール（属性検証モジュール）に対しprop=SS-A-２８、ＩＤが” ３”のサービス制御モジュール（メッセージ設定モジュール）に対しmsg=”Special News available: http://www.yis.co.jp/news/ ２００２０６３０” というように、変更後の電子チケットの属性が提示され、電子バリューハンドラオブジェクトのそれぞれのサービス制御モジュールにおいて検証される。

【００８０】

図１９（ｄ）の場合、電子バリューオブジェクト側のＩＤが” １”のサービス制御モジュール（チケットモジュール）に対しserial= １というように、トランザクション１００５の使用シリアル番号が提示され、電子バリューオブジェクトのチケットモジュールにおいて使用シリアル番号の照合が行われる。

【００８１】

以上のようにして行われる改札決済処理の結果、例えば、図１２に示した電子バリューの場合、可変属性は図２０に示すようになる。特にこの場合、改札決済処理の結果、MESSAGE__２には、”Special News available:http://www.yis.co.jp/news/２００２０６３０” というマーチャントが設定したメッセージが設定され、このメッセージは電子バリューの”Detail”画面表示においてＬＣＤ２００に表示される。また、モバイルユーザ端末１０１とサービスサーバ１０６間の改札決済処理、及びユーザ端末１０７とサービスサーバ１０６間の改札決済処理は、赤外線通信がデジタル無線通信になる以外は同様の手順で行われる。

【００８２】

以上のように、モバイルユーザ端末１０１とサービス端末１０５、及び電子バリューと電子バリューハンドラを構成することにより、各種の改札決済処理、つまり各種の電子バリューを規定することができ、また、安全性を確保しつつ、マーチャントの運用におけるある程度の自由な設定を可能に出来る。

【００８３】

なお、以上に述べた構成では、モバイルユーザ端末１０１とサービス端末１０５との通信に赤外線通信を用いたが、その他の無線通信方式を用いてもよく、その場合、モバイルユーザ端末１０１は赤外線通信モジュール１１１の代わりにその無線通信方式の無線通信手段を、サービス端末１０５は、赤外線通信アダプタ６０２の代わりにその無線通信方式の無線通信手段をそれぞれ備える。また、以上の説明では、モバイル・エレクトロニックコマース・システムを構成するモバイルユーザ端末１０１は、モバイル・エレクトロニックコマース・サービスにおける機能を実現するための、最適なハードウェア構成を備えているが、機能としては、デジタル無線通信機能と、赤外線通信機能、及び、スマートカードリーダーライタと、ディスプレーと、キーボード（または、ペン入力デバイス）と、マイクと、スピーカとを備えたコンピュータによって構成することもできる。この場合、ＦｅＲＡＭ３０１に格納されているプログラムを、パソコンのＯＳ(Operating System)上で動作するソフトウェア・プログラムに変換し、そのソフトウェア・プログラムを、コンピュータから実行可能な場所（例：ハードディスク）に格納しておく。

【００８４】

【発明の効果】

以上のように、第１の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された情報とを備えた電子情報を、保存管理する手段を電子財布に備えたものである。電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

【００８５】

第２の発明は、第１の発明の電子財布に、電子情報から電子情報オブジェクト

を生成し電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００８６】

第３の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の有効性がそれ自身で証明されるので、匿名性が確保される。

【００８７】

第４の発明は、第３の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００８８】

第５の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の発行者が規定する情報を、電子情報に入れることが出来る。

【００８９】

第６の発明は、第５の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００９０】

第７の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された属性情報と、電子情報の発行者によって署名された情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の属性情報の有効性がそれ自身で証明されるので、匿名性が確保される。

【００９１】

第８の発明は、第７の発明の電子財布に、電子情報から電子情報オブジェクト

を生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００９２】

第９の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報の可変の属性情報の有効性がそれ自身で証明されるので、匿名性が確保される。

【００９３】

第１０の発明は、第９の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００９４】

第１１の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示制御情報に署名がされているので、発行者が規定した表示が保証される。

【００９５】

第１２の発明は、第１１の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００９６】

第１３の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示制御情報の識別情報とを備えた電子情報を保存管理する手段を電子財布が備えたものである。表示制御情報の識別情報に署名がされているので、発行者

が規定した表示が保証される。

【００９７】

第１４の発明は、第１３の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【００９８】

第１５の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示リソースの識別情報に署名がされているので、発行者が規定したイメージが保証される。

【００９９】

第１６の発明は、第１５の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【０１００】

第１７の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報及び表示リソースの識別情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。表示制御情報の識別情報および表示リソースの識別情報に署名がされているので、発行者が規定した表示が保証される。

【０１０１】

第１８の発明は、第１７の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【０１０２】

第１９の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報ハンドラの認証鍵によって、電子情報ハンドラを認証することができ、安全性が向上する。

【０１０３】

第２０の発明は、第１９の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【０１０４】

第２１の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報と表示リソースの識別情報及び電子情報ハンドラの認証鍵とを備えた電子情報を保存管理する手段を電子財布に備えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【０１０５】

第２２の発明は、第２１の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【０１０６】

第２３の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報及びサービス制御情報とを備えた電子情報を保存管理する手段を電子財布を備えたものである。サービス制御情報を変更することにより、各種の電子情報を規定することが出来る。

【０１０７】

第２４の発明は、第２３の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【０１０８】

第２５の発明は、固有の秘密鍵とその証明書の組と、その秘密鍵によって署名された可変の属性情報と、電子情報の発行者によって署名された固定の属性情報と表示制御情報の識別情報と表示リソースの識別情報と電子情報ハンドラの認証鍵及びサービス制御情報とを備えた電子情報を保存管理する手段を電子財布に備えたものである。サービス制御情報を変更することにより、各種の電子情報を規定することが出来る。

【０１０９】

第２６の発明は、第２５の発明の電子財布に、電子情報から電子情報オブジェクトを生成し前記電子情報を制御する手段を加えたものである。電子情報オブジェクトが電子情報の変更を行い署名するので、データが増加せず、また安全性が向上する。

【０１１０】

第２７の発明は、サービス制御情報が、少なくとも一つ以上のサービス制御モジュール情報の組合せにしたものである。サービス制御モジュール情報の組合せを変更することにより、各種の電子情報を規定することが出来る。

第２８の発明は、電子情報の電子情報オブジェクトが、決済処理時に交換する各メッセージに、サービス制御情報に基づく決済データを重畳するようにしたものある。決済処理時に交換するメッセージ数を変えること無く、効率的な決済が可能となる。

【０１１１】

第２９の発明は、電子情報の電子情報オブジェクトが、決済処理時に交換する各メッセージに、サービス制御モジュール情報の組合せに基づく決済データを重畳するようにしたものである。決済処理時に交換するメッセージ数を変えること

無く、効率的な決済が可能となる。

【０１１２】

第３０の発明は、電子情報の電子情報オブジェクトが、決済データを重畳するメッセージが、電子情報から電子情報ハンドラに決済処理を申し出るメッセージと、電子情報ハンドラから電子情報に属性値の変更を命令するメッセージと、電子情報から電子情報ハンドラに属性値の変更結果を示すメッセージと、電子情報ハンドラから電子情報への領収書に相当するメッセージであるようにしたものである。各種の電子情報における決済処理を、効率的に行うことが出来る。

【０１１３】

第３１の発明は、電子情報の表示手段を備えるようにしたものであり、電子情報の内容を確認することが出来、ユーザの利便性が向上する。

【０１１４】

第３２の発明は、電子情報から表示情報を生成する手段を備えるものであり、内容が変化した電子情報の内容を確認することが出来、ユーザの利便性が向上する。

【０１１５】

第３３の発明は、第１の発明から第３２の発明に記載の電子財布の処理プログラムを、電子計算機が読み取り可能な形式で記録したものである。これにより、プログラムを、持ち運び可能な形態で、流通させることができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態におけるモバイル・エレクトロニックコマース・システムのブロック構成図

【図２】

（ａ）本発明の実施の形態におけるモバイルユーザ端末の前面の概観図

（ｂ）本発明の実施の形態におけるモバイルユーザ端末の背面の概観図

【図３】

本発明の実施の形態におけるモバイルユーザ端末のブロック構成図

【図４】

本発明の実施の形態におけるモバイルユーザ端末のアプリケーションと他の構成要素と、他の機器との関係を示す模式図

【図５】

（ａ）本発明の実施の形態におけるモバイルユーザ端末の電源オン時の画面の概観図

（ｂ）本発明の実施の形態におけるモバイルユーザ端末のインターネットメニュー画面の概観図

（ｃ）本発明の実施の形態におけるモバイルユーザ端末の電子バリューのオーダー画面の概観図

（ｄ）本発明の実施の形態におけるモバイルユーザ端末のパスワード入力画面の概観図

（ｅ）本発明の実施の形態におけるモバイルユーザ端末の電子バリューの一覧画面の概観図

（ｆ）本発明の実施の形態におけるモバイルユーザ端末の電子バリュー表示画面の概観図

【図６】

本発明の実施の形態におけるサービス端末のブロック構成図

【図７】

本発明の実施の形態におけるユーザ端末のブロック構成図

【図８】

本発明の実施の形態における電子バリューのデータ構造の模式図

【図９】

本発明の実施の形態における電子バリューハンドラーのデータ構造の模式図

【図１０】

本発明の実施の形態における改札決済処理において交換されるメッセージの模式図

【図１１】

（ａ）本発明の実施の形態における改札決済処理のメッセージ、プレゼンテーションのデータ構造の模式図

（ｂ）本発明の実施の形態における改札決済処理のメッセージ、インストラクションのデータ構造の模式図

（ｃ）本発明の実施の形態における改札決済処理のメッセージ、トランザクションのデータ構造の模式図

（ｄ）本発明の実施の形態における改札決済処理のメッセージ、レシートのデータ構造の模式図

（ｅ）本発明の実施の形態における改札決済処理のメッセージ、アクノレッジのデータ構造の模式図

【図１２】

本発明の実施の形態における電子バリューのマークアップ記述言語による記述の模式図

【図１３】

本発明の実施の形態における電子バリューのプレゼンテーションカードと可変属性のマークアップ記述言語による記述の模式図

【図１４】

本発明の実施の形態における電子バリューのサービス制御部とセキュリティ情報部のマークアップ記述言語による記述の模式図

【図１５】

本発明の実施の形態における電子バリューの表示制御部のマークアップ記述言語による記述の模式図

【図１６】

本発明の実施の形態における電子バリューの表示リソース部のマークアップ記述言語による記述の模式図

【図１７】

本発明の実施の形態における電子バリューオブジェクトが生成する"Main"の画面情報の模式図

【図１８】

本発明の実施の形態における電子バリューハンドラのマークアップ記述言語による記述の模式図

【図１９】

（ａ）本発明の実施の形態における改札決済処理のメッセージ、プレゼンテーション中のサービス制御メッセージのデータ構造の模式図

（ｂ）本発明の実施の形態における改札決済処理のメッセージ、インストラクション中のサービス制御メッセージのデータ構造の模式図

（ｃ）本発明の実施の形態における改札決済処理のメッセージ、トランザクション中のサービス制御メッセージのデータ構造の模式図

（ｄ）本発明の実施の形態における改札決済処理のメッセージ、レシート中のサービス制御メッセージのデータ構造の模式図

【図２０】

本発明の実施の形態における改札決済処理後の電子バリューの可変属性のマークアップ記述言語による記述の模式図

【図２１】

（ａ）従来の技術における電子化された価値情報が発行された状態を示す模式図

（ｂ）従来の技術における電子化された価値情報が使用された状態を示す模式図

【符号の説明】

１００　インターネット

１０１　モバイルユーザ端末

１０２　情報提供サーバ端末

１０３　電子バリュー発行サーバ

１０４　決済処理サーバ

１０５　サービス端末

１０６　サービスサーバ

１０７　ユーザ端末

２００　ＬＣＤ

２０１　テンキースイッチ

２０２　終了／電源スイッチ

２０３　通話スイッチ

２０４　ナビゲーションスイッチ

２０５、２０６　ファンクションスイッチ

２０５　レシーバスピーカ

２０６　アンテナ

２０７　マイク

２０９　レシーバスピーカ

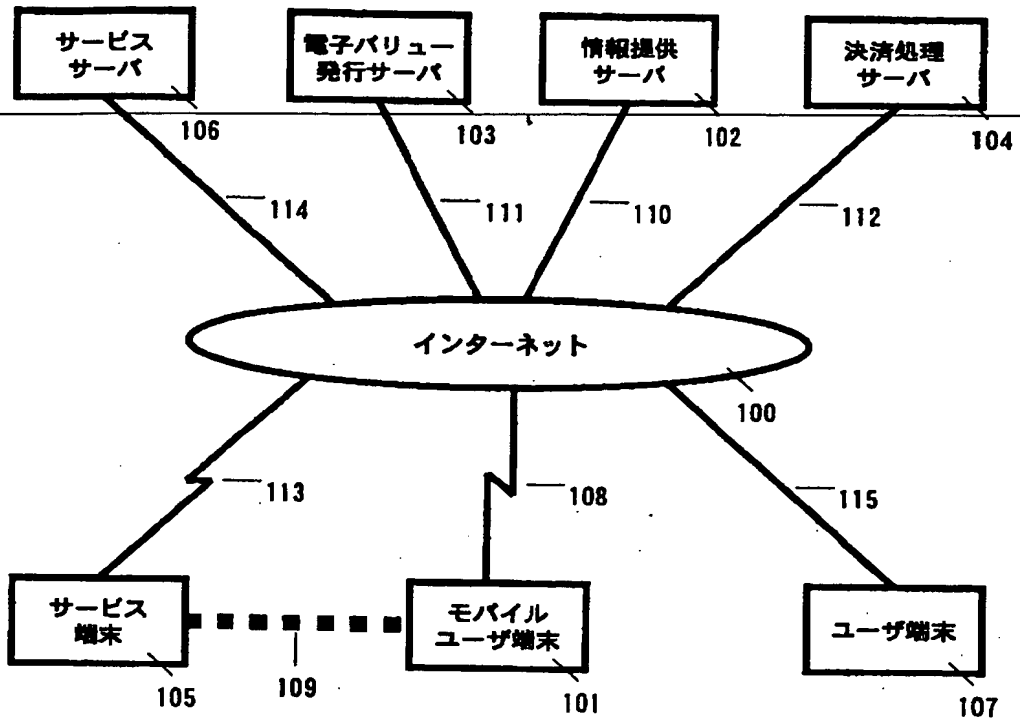
２１０　アンテナ

２１１　赤外線通信ポート（赤外線通信モジュール）

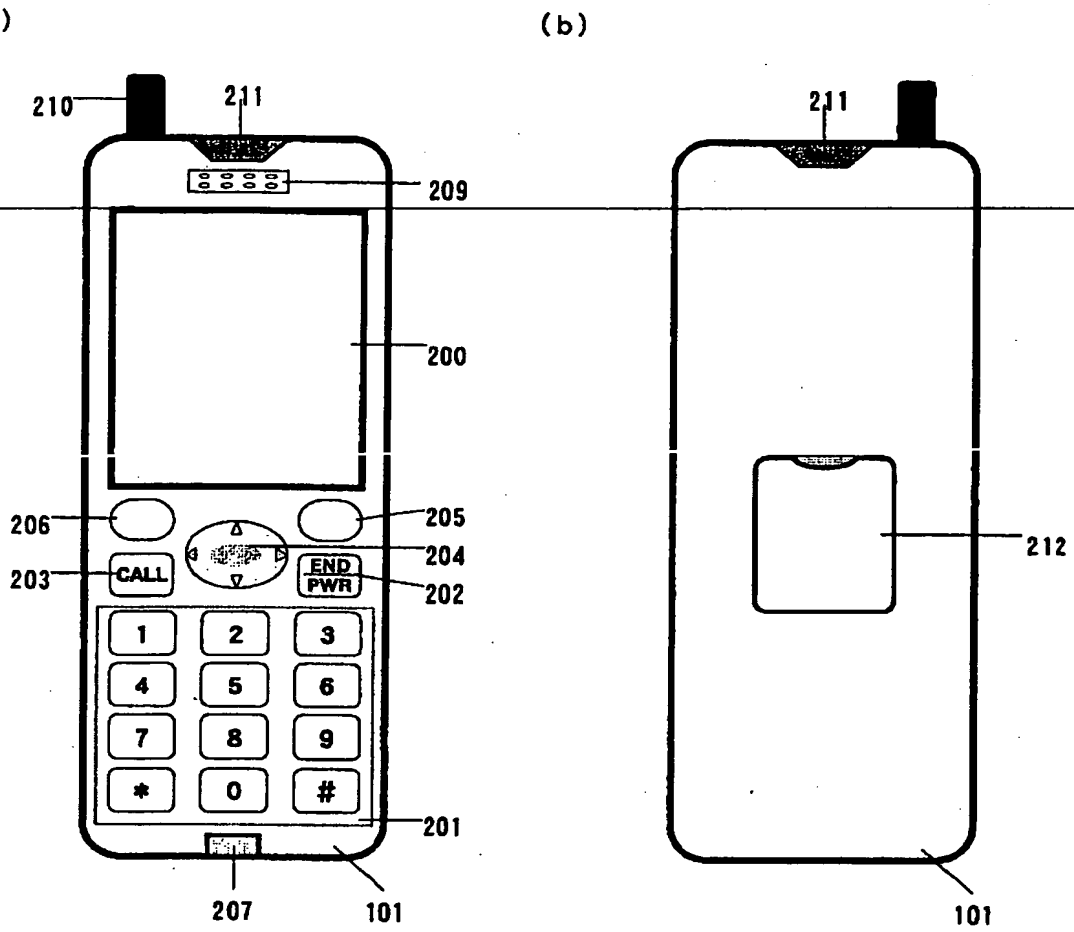
２１２　スマートカードスロット（スマートカードリーダライタ）

【書類名】　　図面

【図１】

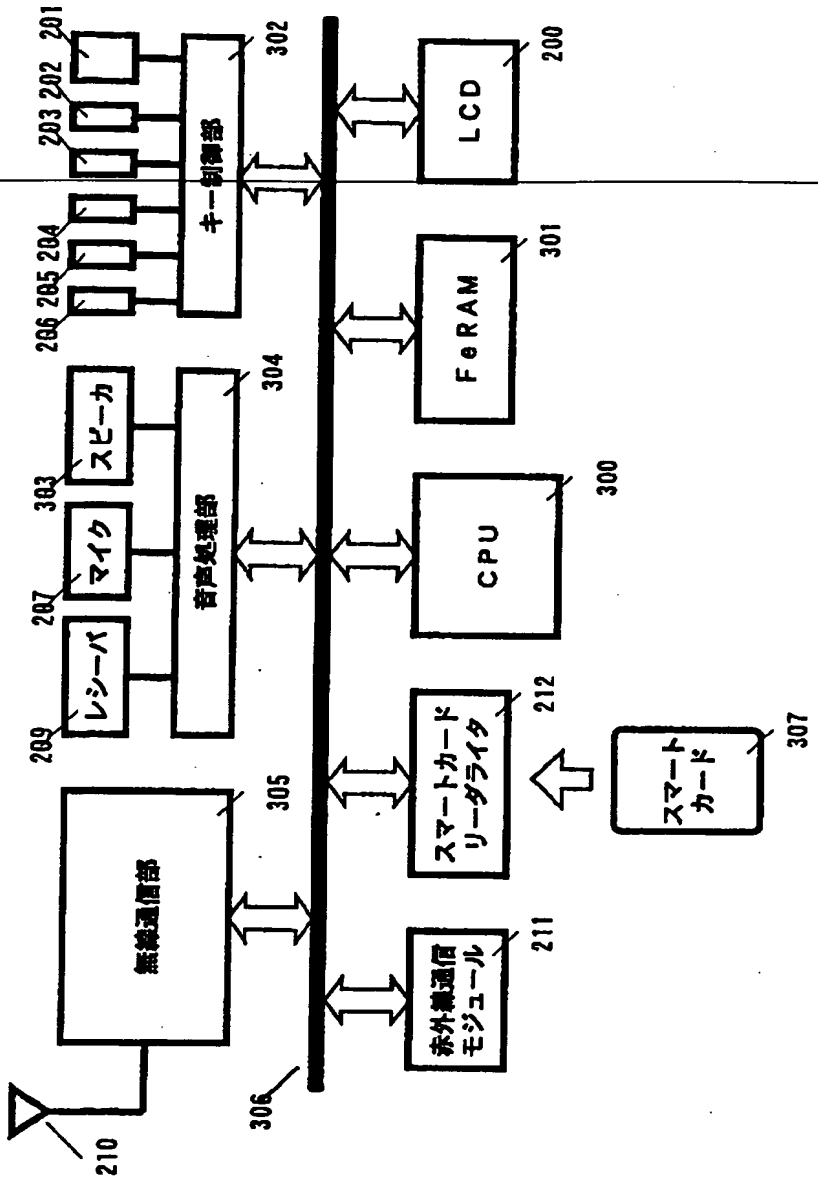

サービス
サーバ
106
電子バリュー
発行サーバ
103
情報提供
サーバ
102
決済処理
サーバ
104
114
111
110
112
インターネット
100
113
108
115
サービス
端末
105
109
モバイル
ユーザ端末
101
ユーザ端末
107

【図２】

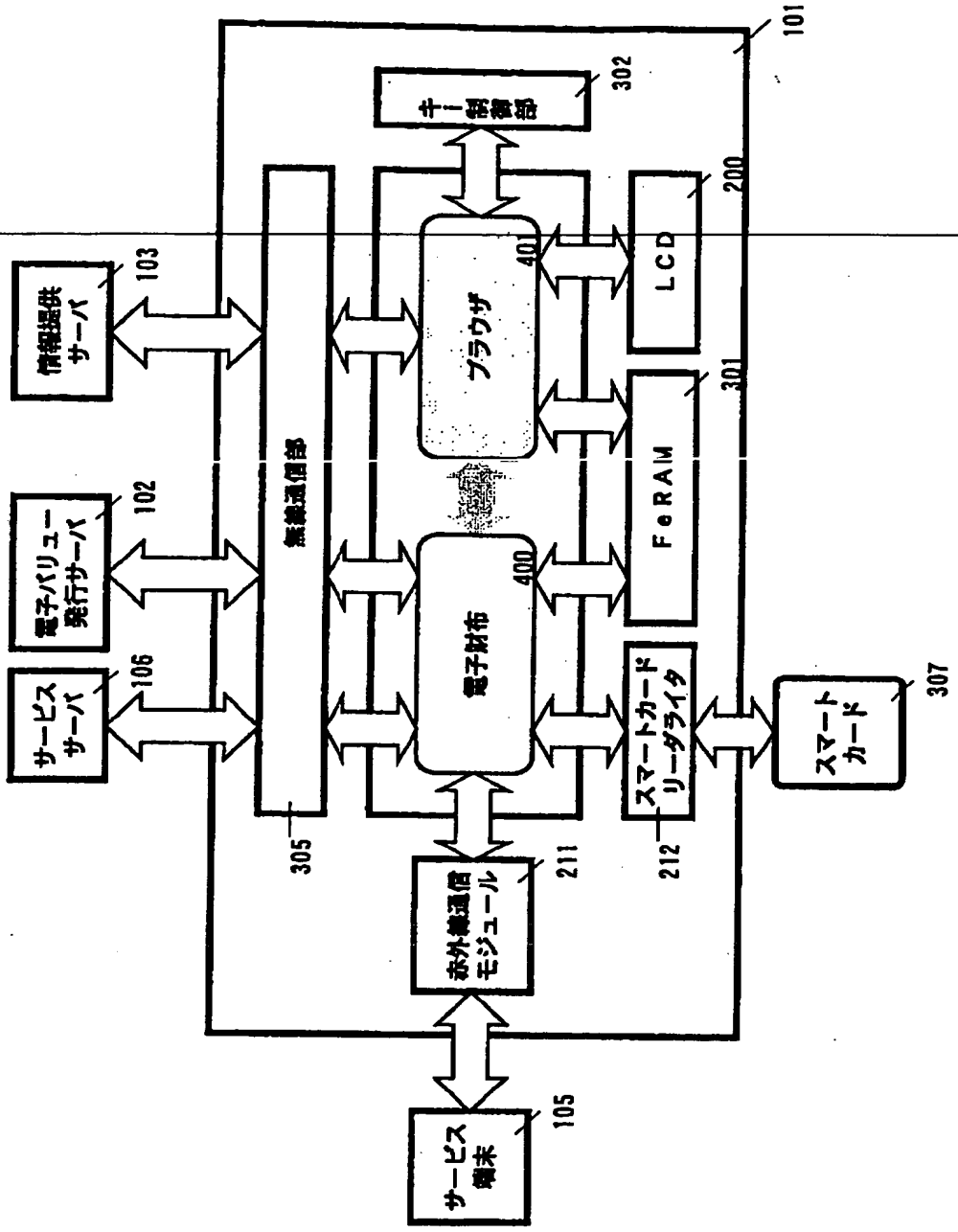


出証特２０００－３０７５４７６

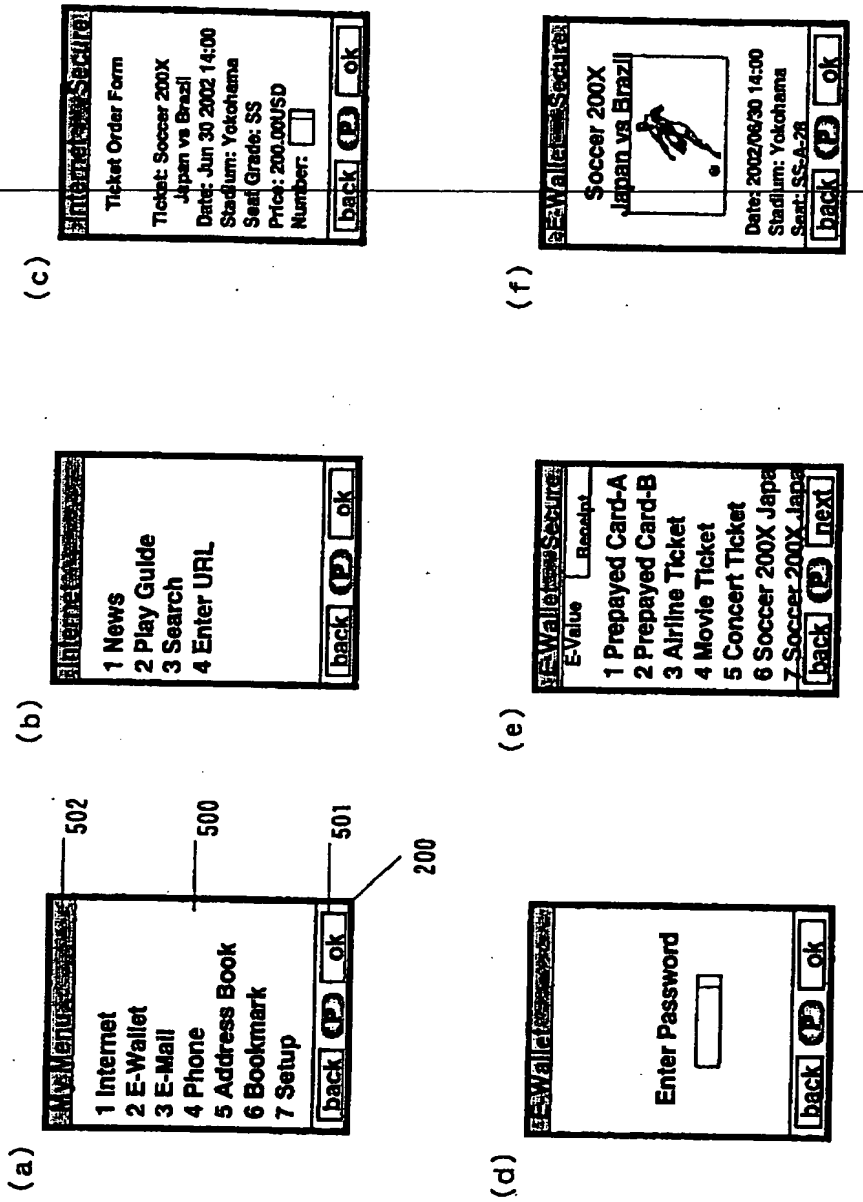
【図３】


201
202
203
204
205
206
キー制御部
302
LCD
200
FeRAM
301
スピーカ
303
マイク
287
レシーバ
289
音声処理部
304
CPU
300
スマートカード
リーダライタ
212
スマート
カード
307
無線通信部
305
赤外線通信
モジュール
211
210
306

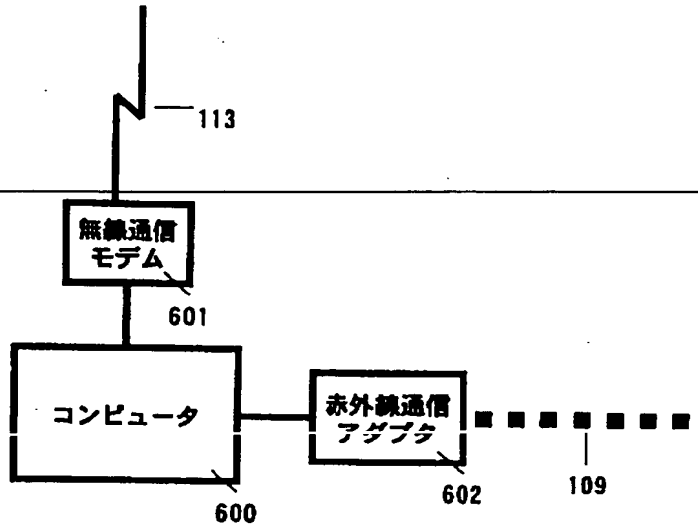
【図４】


101
302
200
401
ブラウザ
LCD
103
情報提供サーバ
301
FeRAM
102
電子バリュー発行サーバ
400
電子財布
106
サービスサーバ
スマートカードリーダライタ
307
スマートカード
305
211
212
赤外線通信モジュール
105
サービス端末

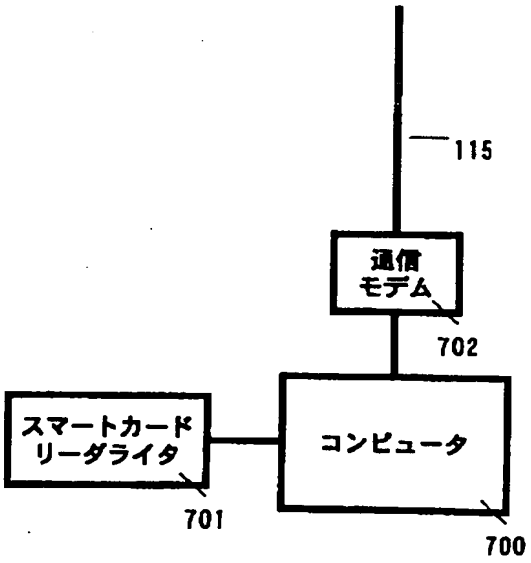
【図５】


(a)
MyMenu
1 Internet
2 E-Wallet
3 E-Mail
4 Phone
5 Address Book
6 Bookmark
7 Setup
back
ok
502
500
501
200
(b)
Internet
1 News
2 Play Guide
3 Search
4 Enter URL
back
ok
(c)
Internet
Ticket Order Form
Ticket: Soccer 200X
Japan vs Brazil
Date: Jun 30 2002 14:00
Stadium: Yokohama
Seat Grade: SS
Price: 200.00USD
Number:
back
ok
(d)
E-Wallet
Enter Password
back
ok
(e)
E-Wallet
E-Value
Receipt
1 Prepayed Card-A
2 Prepayed Card-B
3 Airline Ticket
4 Movie Ticket
5 Concert Ticket
6 Soccer 200X Japa
7 Soccer 200X Japa
back
next
(f)
E-Wallet
Soccer 200X
Japan vs Brazil
Date: 2002/06/30 14:00
Stadium: Yokohama
Seat: SS-A-26
back
ok

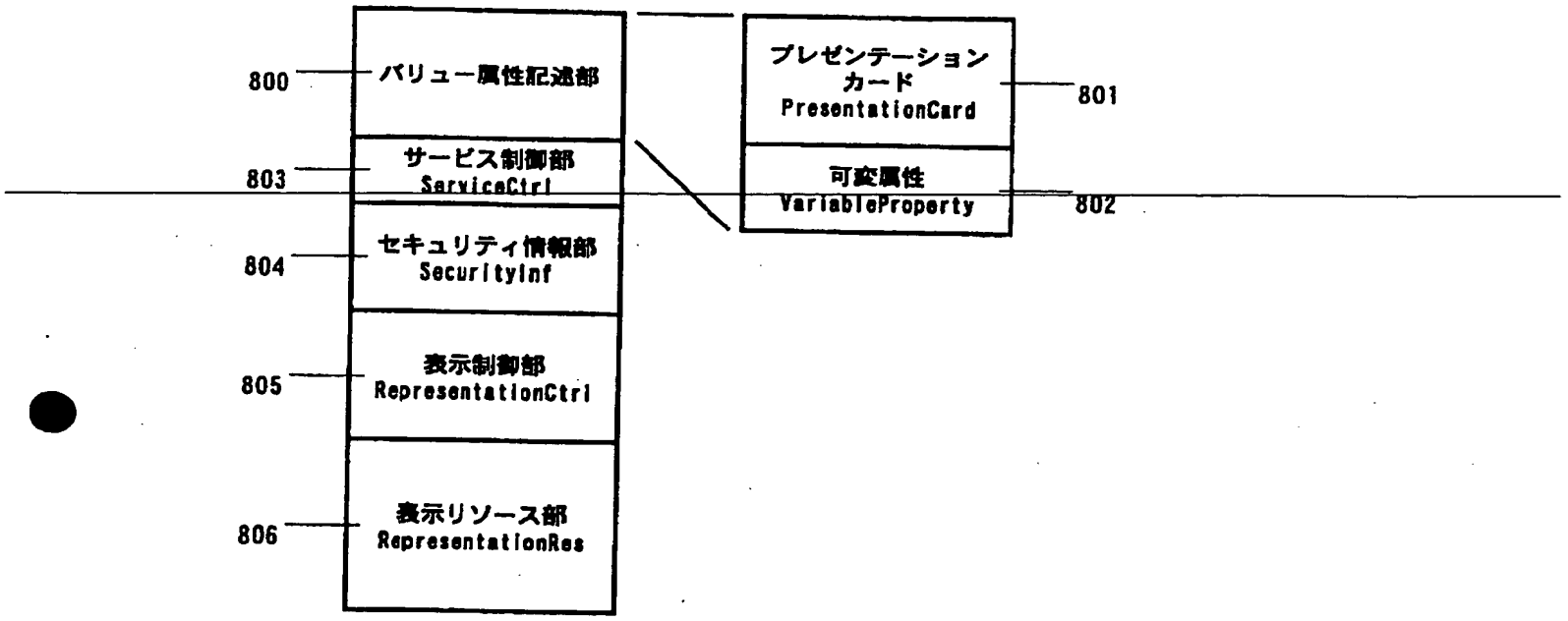
【図６】


113
無線通信
モデム
601
コンピュータ
600
赤外線通信
アダプタ
602
109

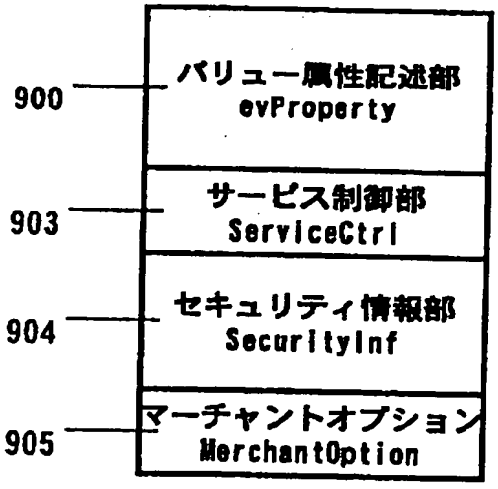
【図７】


115
通信
モデム
702
スマートカード
リーダライタ
701
コンピュータ
700

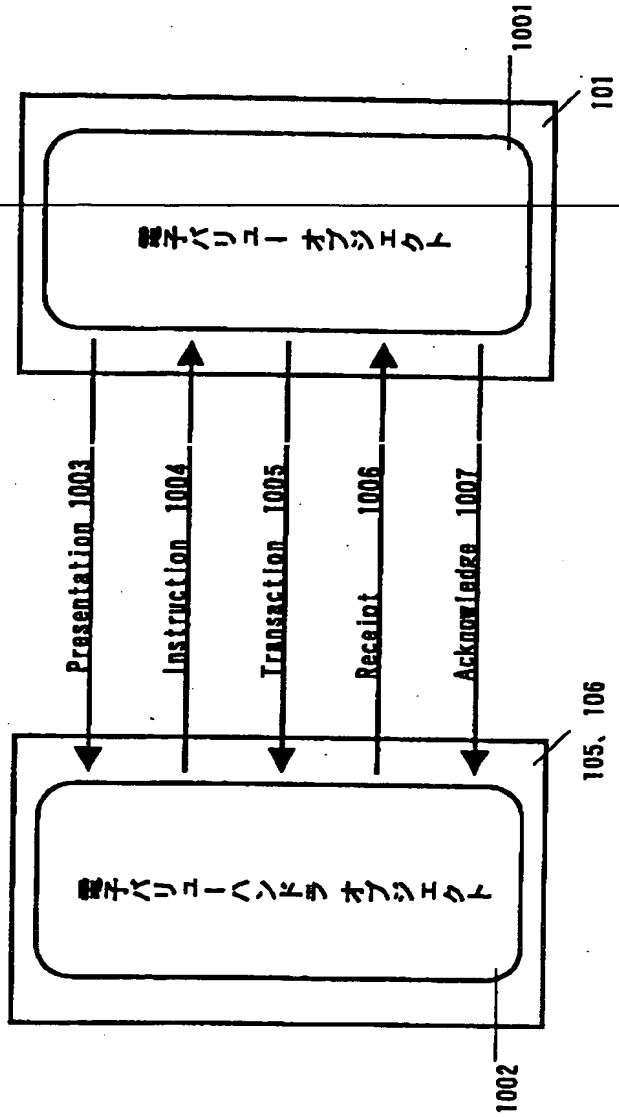
【図８】


800
バリュー属性記述部
803
サービス制御部
ServiceCtrl
804
セキュリティ情報部
SecurityInf
805
表示制御部
RepresentationCtrl
806
表示リソース部
RepresentationRes
プレゼンテーション
カード
PresentationCard
801
可変属性
VariableProperty
802

【図９】

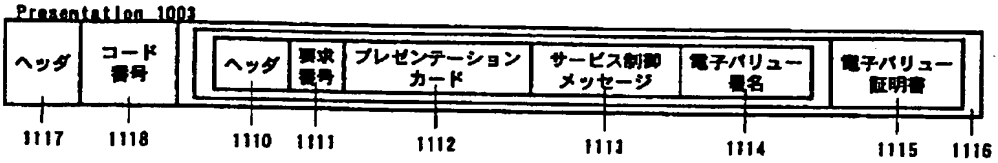

900
バリュー属性記述部
evProperty
903
サービス制御部
ServiceCtrl
904
セキュリティ情報部
SecurityInf
905
マーチャントオプション
MerchantOption

【図１０】

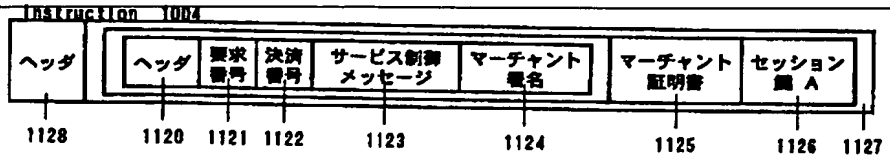

1001
101
Presentation 1003
Instruction 1004
Transaction 1005
Receipt 1006
Acknowledge 1007
105、106
1002

【図１１】

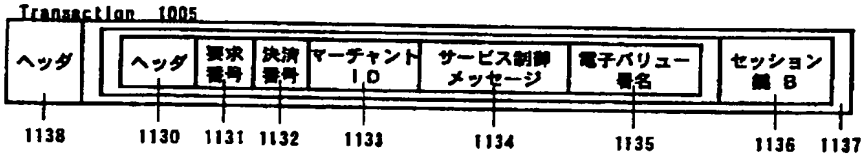
(a)


Presentation 1003
ヘッダ
コード番号
ヘッダ
要求番号
プレゼンテーションカード
サービス制御メッセージ
電子バリュー署名
電子バリュー証明書
1117
1118
1110
1111
1112
1113
1114
1115
1116

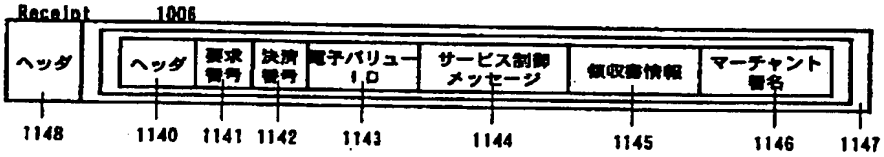
(b)


Instruction 1004
ヘッダ
ヘッダ
要求番号
決済番号
サービス制御メッセージ
マーチャント署名
マーチャント証明書
セッション鍵 A
1128
1120
1121
1122
1123
1124
1125
1126
1127

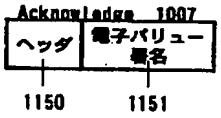
(c)


Transaction 1005
ヘッダ
ヘッダ
要求番号
決済番号
マーチャントID
サービス制御メッセージ
電子バリュー署名
セッション鍵 B
1138
1130
1131
1132
1133
1134
1135
1136
1137

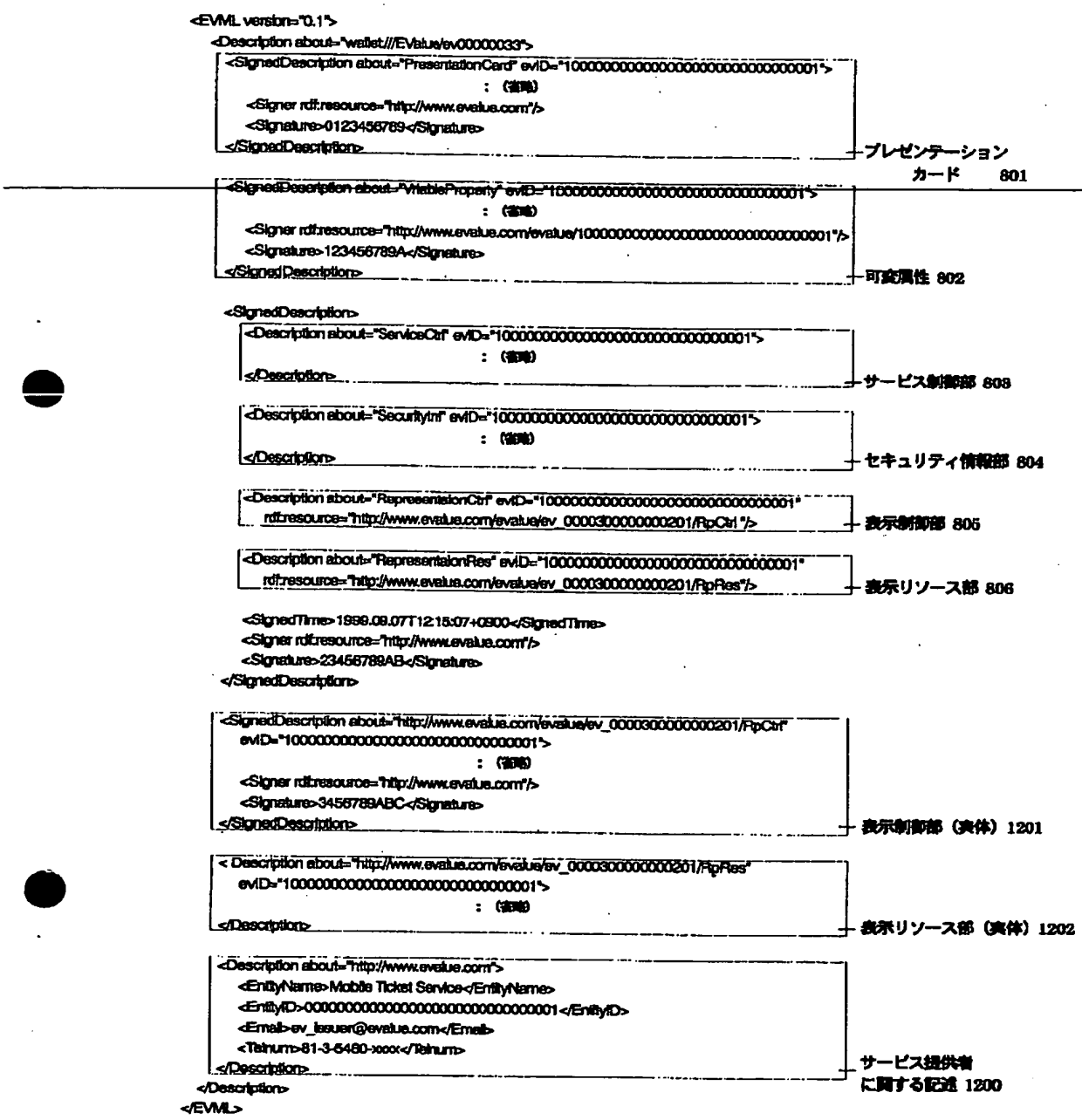
(d)


Receipt 1006
ヘッダ
ヘッダ
要求番号
決済番号
電子バリューID
サービス制御メッセージ
領収書情報
マーチャント署名
1148
1140
1141
1142
1143
1144
1145
1146
1147

(e)


Acknowledge 1007
ヘッダ
電子バリュー署名
1150
1151

【図１２】


<EVML version="0.1">
<Description about="wallet:///EValue/ev00000033">
<SignedDescription about="PresentationCard" evID="10000000000000000000000000000001">
: (省略)
<Signer rdf:resource="http://www.evalue.com"/>
<Signature>0123456789</Signature>
</SignedDescription>
プレゼンテーション
カード 801
<SignedDescription about="VriableProperty" evID="10000000000000000000000000000001">
: (省略)
<Signer rdf:resource="http://www.evalue.com/evalue/10000000000000000000000000000001"/>
<Signature>123456789A</Signature>
</SignedDescription>
可変属性 802
<SignedDescription>
<Description about="ServiceCtrl" evID="10000000000000000000000000000001">
: (省略)
</Description>
サービス制御部 803
<Description about="SecurityInf" evID="10000000000000000000000000000001">
: (省略)
</Description>
セキュリティ情報部 804
<Description about="RepresentationCtrl" evID="10000000000000000000000000000001"
rdf:resource="http://www.evalue.com/evalue/ev_0000300000000201/RpCtrl"/>
表示制御部 805
<Description about="RepresentationRes" evID="10000000000000000000000000000001"
rdf:resource="http://www.evalue.com/evalue/ev_0000300000000201/RpRes"/>
表示リソース部 806
<SignedTime>1999.09.07T12:15:07+0900</SignedTime>
<Signer rdf:resource="http://www.evalue.com"/>
<Signature>23456789AB</Signature>
</SignedDescription>
<SignedDescription about="http://www.evalue.com/evalue/ev_0000300000000201/RpCtrl"
evID="10000000000000000000000000000001">
: (省略)
<Signer rdf:resource="http://www.evalue.com"/>
<Signature>3456789ABC</Signature>
</SignedDescription>
表示制御部（実体）1201
< Description about="http://www.evalue.com/evalue/ev_0000300000000201/RpRes"
evID="10000000000000000000000000000001">
: (省略)
</Description>
表示リソース部（実体）1202
<Description about="http://www.evalue.com">
<EntityName>Mobile Ticket Service</EntityName>
<EntityID>00000000000000000000000000000001</EntityID>
<Email>ev_issuer@evalue.com</Email>
<Telnum>81-3-5480-xxxx</Telnum>
</Description>
サービス提供者
に関する記述 1200
</Description>
</EVML>

【図１３】

```
<SignedDescription about="PresentationCard" evID="10000000000000000000000000000001">
   <evType>ticket</evType>
   <evCode>0000300000000201</evCode>
   <evID>10000000000000000000000000000001</evID>
   <evName>Soccer 200X Ticket</evName>
   <evConditionBitmap>0000000000000001</evConditionBitmap>
   <evProp name="TITLE" value="Soccer 200X Japan vs Brazil"/>
   <evProp name="DATE" value="2002.06.30T14:00+0900"/>
   <evProp name="GATE_OPEN" value="2002.06.30T10:00+0900"/>
   <evProp name="LOCATION_NAME" value="Yokohama"/>
   <evProp name="LOCATION_URI" value="http://www.yis.co.jp/map"/>
   <evProp name="SEAT_NUM" value="SS-A-28"/>
   <evProp name="SEAT_POS" value="http://www.mts.com/ticket123/seat/SS-A-28"/>
   <evProp name="SPONSOR_NAME" value="WORLD FOOTBALL ASSOCIATION"/>
   <evProp name="SPONSOR_URI" value="http://www.wfa.org"/>
   <evProp name="CONTACT_TELNUM" value="+81-3-5460-xxxx"/>
   <evProp name="CONTACT_URI" value="http://www.mts.com/contact"/>
   <evProp name="ISSUER_NAME" value="Mobile Ticket Service"/>
   <evProp name="ISSUER_URI" value="http://www.mts.com"/>
   <evProp name="MESSAGE_1" value="No Dangerous  Objects"/>
   <SignedTime>1999.09.07T12:15:07+0900</SignedTime>
   <Signer rdf:resource="http://www.evalue.com"/>
   <Signature>0123456789</Signature>
</SignedDescription>

<SignedDescription about="VriableProperty" evID="10000000000000000000000000000001">
   <evFlag VALIDITY=1 USED=0/>
   <evProp name="USE_SERIAL" value=0/>
   <evProp name="NUMBER" value=1/>
   <evProp name="START_VALID" value="1999.07.23T00:00+0900"/>
   <evProp name="END_VALID" value="2002.06.30T23:59+0900"/>
   <evProp name="MESSAGE_2" value=/>
   <SignedTime>1999.09.07T12:15:07+0900</SignedTime>
   <Signer rdf:resource="http://www.evalue.com/evalue/10000000000000000000000000000001"/>
   <Signature>123456789A</Signature>
</SignedDescription>
```

【図１４】

```
<Description about="ServiceCtrl" evID="10000000000000000000000000000001">
  <SC-module type="ticket" ID=1 number=$NUMBER start=$START_VALID end=$END_VALID
    used_flag=$USED validity_flag=$VALIDITY serial=$USE_SERIAL/>
  <SC-module type="verify_prop" ID=2 prop=$SEAT_NUM/>
  <SC-module type="set_message" ID=3 msg=$MESSAGE_2/>
</Description>
```

```
<Description about="SecurityInf" evID="10000000000000000000000000000001">
  <evOwner>
    <Description about="http://www.evalue.com/user/11000000000000000000000000000001"
      EntityName="Taro Suzuki"
      EntityID="11000000000000000000000000000001"/>
  </evOwner>
  <evResource>http://www.evalue.com/evalue/10000000000000000000000000000001</evResource>
  <evCertificate>
    0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF
  </evCertificate>
  <evPrivateKey>0123456789</evPrivateKey>
  <evAuthKey>0123456789ABCDEF</evAuthKey>
  <evhandlerAuthKey>ABCDEF0123456789</evhandlerAuthKey>
</Description>
```

【図１５】

```
<SignedDescription about="http://www.evalue.com/evalue/ev_0000300000000201/RpCtrl"
  evID="10000000000000000000000000000001">
  <OptimumRpCtrl>
    <Description about="http://www.evalue.com/evalue/ev_0000300000000201/RpCtrl_M01">
      < RpType>MOBILE 01</RpType>
      < RepresentaionCtrlData>
        <CARD name="Main">
          <HAEAD>
            <TITLE><evP>$TITLE</evP></TITLE>
          </HAEAD>
          <BODY>
          <Do type="ACCEPT">
            <Go HREF="wallet:///evTransact"/>
          </Do>
          <CENTER><H1><evP>$TITLE</evP></H1></CENTER>
          <BR><CENTER><IMG SRC="wallet:///evResource label=MAIN_IMG"></CENTER>
          <BR><UL>Date:<evP>$DATE</evP>
          <BR>Stadium:<A HREF=<evP>$LOCATION_URI</evP>><evP>$LOCATION_NAME</evP></A>
          <BR>Seat:<A HREF=<evP>$SEAT_POS</evP>><evP>$SEAT_NUM</evP></A>
          <BR><A HREF="Detail">Details</A></UL>
          </BODY>
        </CARD>
        <CARD name="Detail">
          <HAEAD>
            <TITLE><evP>$TITLE</evP></TITLE>
          </HAEAD>
          <BODY>
          <Do type="ACCEPT">
            <Go HREF="wallet:///evTransact"/>
          </Do>
          <CENTER><H1><evP>$TITLE</evP></H1></CENTER>
          <BR><UL>Date:<evP>$DATE</evP>
          <BR>Open Gate:<evP>$GATE_OPEN</evP>
          <BR>Stadium:<A HREF=<evP>$LOCATION_URI</evP>><evP>$LOCATION_NAME</evP></A>
            <BR><A HREF="wallet:///evResource label=MAP">Map</A>
          <BR>Seat:<A HREF=<evP>$SEAT_POS</evP>><evP>$SEAT_NUM</evP></A>
          <BR>Term of Validity: <evV>$START_VALID</evV> - <evV>$END_VALID</evV>
          <BR>Sponsor:<A HREF=<evP>$SPONSOR_URI</evP>><evP>$SPONSOR_NAME</evP></A>
          <BR>Contact:<A HREF="telephone:///dial num=<evP>$CONTACT_TELNUM</evP>">
            <evP>$CONTACT_TELNUM</evP></A>
          <BR>Issuer:<A HREF=<evP>$ISSUER_URI</evP>><evP>$ISSUER_NAME</evP></A>
          <BR><evP>$MESSAGE_1</evP>
          <BR><evV>$MESSAGE_2</evV>
          <BR><A HREF="Main">Top Page</A></UL>
          </BODY>
        </CARD>
      </RpresentaionCtrlData>
    </Description>
  </OptimumRpCtrl>
  <SignedTime>1999.09.07T12:15:07+0900</SignedTime>
  <Signer rdf:resource="http://www.evalue.com"/>
  <Signature>3456789ABC</Signature>
</SignedDescription>
```

【図１６】

```
< Description about="http://www.evalue.com/evalue/ev_0000300000000201/RpRes"
   evID="10000000000000000000000000000001">
   <OptimumRpRes>
      <Image>
         URI="http://www.evalue.com/resources/0123456789ABCDEF"
         label="MAIN_IMG"
         type="jpeg"
         data="1202A846574A63D946B48364605987F687543"
      </Image>
      <Image>
         URI="http://www.evalue.com/resources/123456789ABCDEF0"
         label="MAP"
         type="jpeg"
         data="202A846574A63D946B48364605987F687543F"
      </Image>
      <Sound>
         URI="http://www.evalue.com/resources/23456789ABCDEF01"
         label="Greet"
         type="mp3"
         data="1202A846574A63D946B48364605987F687543"
      </Sound>
   </OptimumRpRes>
</Description>
```

【図１７】

```
< :VML version="0.1">
   <CARD name="Main">
      <HAEAD>
         <TITLE>Soccer 200X Japan vs Brazil </TITLE>
      </HAEAD>
      <BODY>
         <Do type="ACCEPT">
            <Go HREF="wallet:///evTransact"/>
         </Do>
         <CENTER><H1>Soccer 200X Japan vs Brazil </H1></CENTER>
         <BR><CENTER><IMG SRC="wallet:///evResource label=MAIN_IMG"></CENTER>
         <BR><UL>Date: 2002.06.30T14:00+0900
         <BR>Stadium:<A HREF="http://www.yis.co.jp/map"> Yokohama </A>
         <BR>Seat:<A HREF="http://www.mts.com/ticket123/seat/SS-A-28"> SS-A-28</A>
         <BR><A HREF="Detail">Details</A></UL>
      </BODY>
   </CARD>
< :VML>
```

【図１８】

```
<EVML version="0.1">
  <Description about="evMerchant://evHandler/evh00000001">
    <SignedDescription>
      <Description about="evProperty" evhandlerID="20000000000000000000000000000001">
        <evType>ticket</evType>
        <evCode>0000300000000201</evCode>
        <evhandlerID>20000000000000000000000000000001</evhandlerID>
        <evName>Soccer 200X Ticket</evName>
        <evConditionBitmap>0000000000000001</evConditionBitmap>
        <evProp name="TITLE" value="Soccer 200X Japan vs Brazil"/>
        <evProp name="DATE" value="2002.06.30T14:00+0900"/>
        <evProp name="GATE_OPEN" value="2002.06.30T10:00+0900"/>
        <evProp name="LOCATION_NAME" value="Yokohama"/>
        <evProp name="LOCATION_URI" value="http://www.yts.co.jp/map"/>
        <evProp name="SEAT_NUM" value= permission="public"/>
                                  : (省略)
        <evProp name="MESSAGE_2" value= permission="public"/>
      </Description>                                          ―バリュー属性記述部 900
      <Description about="ServiceCtrl" evhandlerID="20000000000000000000000000000001">
        <SC-module type="ticket" ID=1 number=$NUMBER start=$START_VALID end=$END_VALID
          used_flag=$USED validity_flag=$VALIDITY serial=$USE_SERIAL />
        <SC-module type="verify_prop" ID=2 prop=$SEAT_NUM/>
        <SC-module type="set_message" ID=3 msg=$MESSAGE_2/>
      </Description>                                          ―サービス制御部 903
      <Description about="SecurityInf" evhandlerID="20000000000000000000000000000001">
        <evhandlerOwner>
          <Description about="http://www.evalue.com/merchant/21000000000000000000000000000001"
            EntityName="ABC Event Service"
            EntityID="21000000000000000000000000000001"/>
        </evhandlerOwner>
        <evResource>http://www.evalue.com/evhandler/20000000000000000000000000000001
        </evResource>
        <evAuthKey>0123456789ABCDEF</evAuthKey>
        <evhandlerAuthKey>ABCDEF0123456789</evhandlerAuthKey>
      </Description>                                          ―セキュリティ情報部 904
      <SignedTime>1999.09.07T12:15:07+0900</SignedTime>
      <Signer>
        <Description about="http://www.evalue.com">
          <EntityName>Mobile Ticket Service</EntityName>
          <EntityID>00000000000000000000000000000001</EntityID>
          <Email>ev_issuer@evalue.com</Email>
          <Telnum>81-3-5480-xxxx</Telnum>
        </Description>
      </Signer>
      <Signature>23456789AB</Signature>
    </SignedDescription>
    <Description about="MerchantOption" evhandlerID="20000000000000000000000000000001">
      <SetevProp>$SEAT_NUM="SS-*-*"</SetevProp>
      <SetevProp>$MESSAGE_2="Special News available: http://www.yts.co.jp/news/20020630"
      </SetevProp>
    </Description>                                            ―マーチャントオプション
  </Description>                                                  905
</EVML>
```

【図１９】

a)

```
<SC-MSG>
  <scm_msg ID=1 number=1 start="1999.07.23T00:00+0900" end="2002.06.30T23:59+0900"
    used_flag=0 validity_flag=1 serial=0/>
  <scm_msg ID=2 prop="SS-A-28"/>
  <scm_msg ID=3 msg=/>
</SC-MSG>
```

b)

```
<SC-MSG>
  <scm_msg ID=1 number=0 start="2002.06.30T12:25+0900" end="2002.06.30T23:59+0900"
    used_flag=1 validity_flag=1 serial=1/>
  <scm_msg ID=3 msg="Special News available: http://www.yis.co.jp/news/20020630"/>
</SC-MSG>
```

c)

```
<SC-MSG>
  <scm_msg ID=1 number=0 start="2002.06.30T12:25+0900" end="2002.06.30T23:59+0900"
    used_flag=1 validity_flag=1 serial=1/>
  <scm_msg ID=2 prop="SS-A-28"/>
  <scm_msg ID=3 msg="Special News available: http://www.yis.co.jp/news/20020630"//>
</SC-MSG>
```

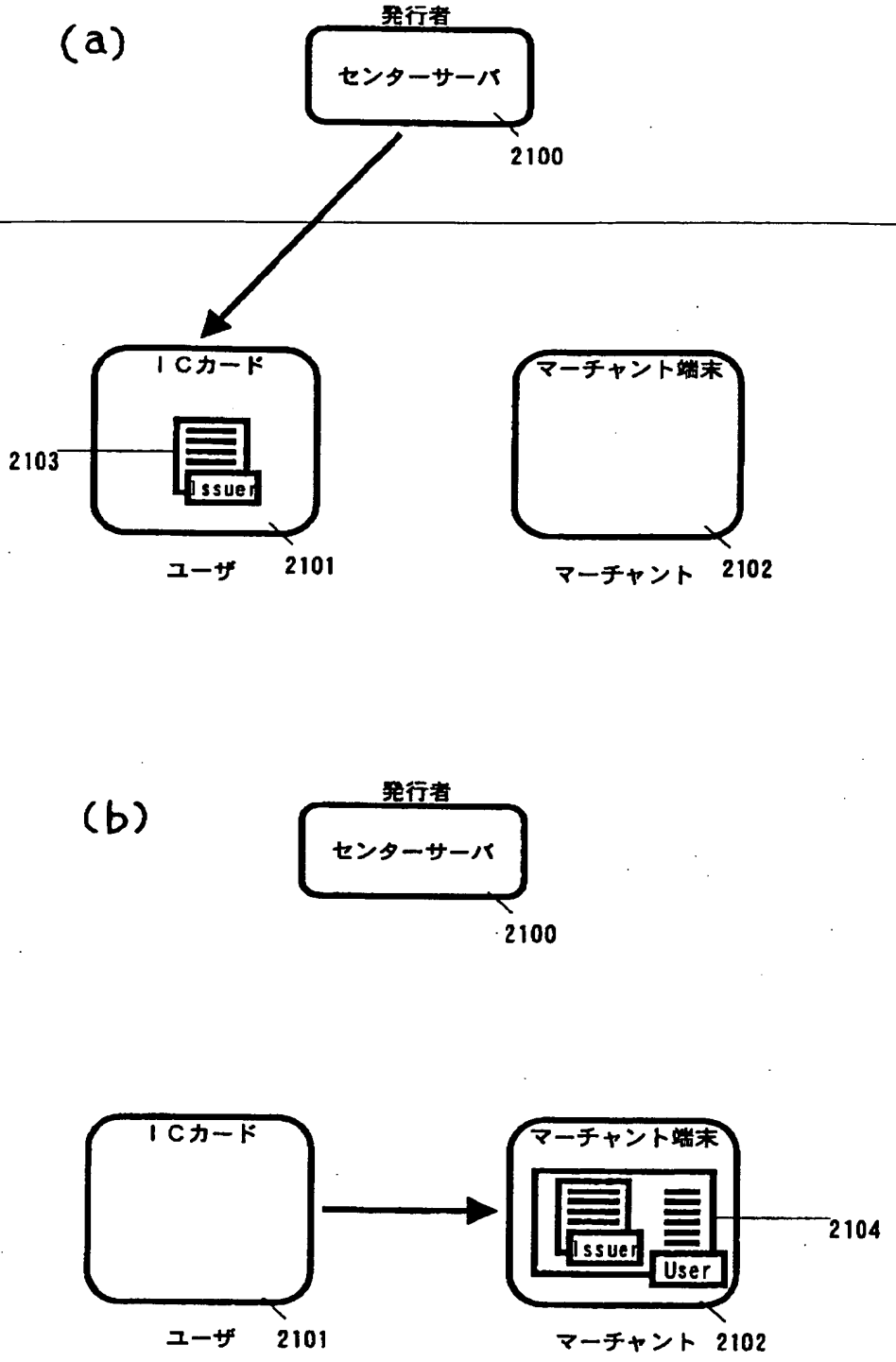
d)

```
<SC-MSG>
    <scm_msg ID=1 serial=1/>
</SC-MSG>
```

【図２０】

```
<SignedDescription about="VriableProperty" evID="10000000000000000000000000000001">
  <evFlag VALIDITY=1 USED=1/>
  <evProp name="USE_SERIAL" value=1/>
  <evProp name="NUMBER" value=0/>
  <evProp name="START_VALID" value="2002.06.30T12:25+0900"/>
  <evProp name="END_VALID" value="2002.06.30T23:59+0900"/>
  <evProp name="MESSAGE_2" value="Special News available: http://www.yis.co.jp/news/20020630"/>
  <SignedTime>2002.06.30T12:25+0900</SignedTime>
  <Signer rdf:resource="http://www.evalue.com/evalue/10000000000000000000000000000001"/>
  <Signature>A12345678A</Signature>
</SignedDescription>
```

【図２１】


(a)
発行者
センターサーバ
2100
ＩＣカード
2103
Issuer
ユーザ
2101
マーチャント端末
マーチャント
2102
(b)
発行者
センターサーバ
2100
ＩＣカード
ユーザ
2101
マーチャント端末
Issuer
User
2104
マーチャント
2102

【書類名】要約書

【要約】

【課題】　匿名性と安全性、および利便性に優れ、価値情報の効率的な電子化と、各種の電子化された価値情報をユーザが効率的に取り扱うことが出来る電子財布を提供することを目的とする。

【解決手段】　電子バリューの固定属性を示すプレゼンテーションカード８０１は、サービス提供者によりデジタル署名されており、可変属性８０２は、この電子バリューの秘密鍵によってデジタル署名されている。また、サービス制御部８０３とセキュリティ情報部８０４と表示制御部８０５と表示リソース部８０６は、サービス提供者によりデジタル署名されている。これらのデジタル署名は、電子バリューオブジェクトが生成される度に検証される。

【選択図】図８

出　願　人　履　歴　情　報

識別番号　〔０００００５８２１〕

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社